Politecnico di Torino

Politecnico di Torino

Corso di Laurea in INGEGNERIA ENERGETICA E NUCLEARE

A.a. 2021/2022

Sessione di Laurea Dicembre 2022

Blockchain as a turning-point innovation: Energy consumption and socioeconomic evaluation

Supervisors:
Vittorio Verda
Salvatore Manco'

Candidate:
Matteo Taviani

Abstract

Blockchain technology, particularly with the advent of Bitcoin, has developed and taken hold in many application domains. It is hailed as a profoundly innovative technology, capable of transforming the use of data through decentralization. Another strength of blockchain is its transparency and security, intrinsic to the design of the technology itself. Conversely, its consumption is also intrinsic to the design of the technology itself; the way it is built, it employs a consensus mechanism used to reach the necessary agreement on a single data value or network state between distributed processes or multi-agent systems. Hence, it brings with it a large consumption of electricity with consequent negative effects on the environmental impact. This research aims at the general study of blockchain by attempting to touch upon all thesensitive areas in which it is used: the financial, the socio-economic, but above all the energy sectors.

Contents

1. Introduction

The 'blockchain' is the innovative result of combining numerous existing technological components. Particularly, the famously unknown figure Satoshi Nakamoto, who presented Bitcoin's foundations, facilitated the growth of this new technology through what is still the most successful cryptocurrency in existence today. As we will see later, the creative combination of cryptographic hashes, consensus methods, and Merkle trees has produced an innovation with great promise.

The blockchain enabled Bitcoin (we will analyze the structure and technology of the blockchain by referring to the cryptocurrency Bitcoin, which enabled the development of the technology itself) to become the first secure digital currency, capable of preventing duplicate spending without the need for a central authority in which all players have confidence. As a result, Bitcoin has been able to establish itself globally with relative ease, function effectively as a means of holding and transferring value and continue to expand rapidly. Its transactions are immutable, transparent, and verifiable by anyone, despite being entirely decentralized and lacking a central authority. However, it quickly became apparent that the properties of blockchain technology make it suitable for numerous other application areas besides cryptocurrencies. It can be used to guarantee secure, transparent, and unchangeable financial transactions. In addition, technological advancements have given rise to so-called 'smart contracts' which, as we shall see, have

far more revolutionary impacts than cryptocurrency. However, a substantial amount of energy is required, which derives from the revolutionary technology itself, especially the Proof-of-Work consensus procedures that guarantee the integrity and immutability of transactions. Furthermore, as this technology spreads, its impact on energy usage will increase.

1.1 Scope and structure of the study

The study aims at analyzing blockchain technology by looking at all the sensitive issues that are related to it.

The research is structured as follows: Section 2 is an introduction of the technology and how it works (blockchain structure, distributed ledger, blockchain system, consensus mechanisms, underlining its innovative importance and the considerable impact it can have on a multiplicity of application domains. These will be analyzed in Section 3, where Bitcoin, smart contracts, NFTs and other application domains will be discussed. Section 4 will be dedicated to the financial focus, the 'challenge' cryptocurrencies pose to traditional finance (introduction of DeFi) and regulations in different countries. Qualitative and quantitative analysis of blockchain consumption will take center stage in Section 5. Finally, discussions on the socio-economic aspects of blockchain innovation will be addressed in Section 6.

2. Focus on Innovation: Blockchain technology

Schumpeter was one of the first economists to deal with the subject of innovation in a broad and comprehensive manner, attempting to define this phenomenon through a number of theories. He starts from a dynamic conception of the economy "as a distinct phenomenon, completely unrelated to what can be observed in the circular flow and tendency towards equilibrium". According to the dynamic conception, innovation is the result of evolution and industrial change that bring to a new competitive environment.

The *Disruptive Innovation* theory was coined by Christensen when he first studied the reasons why a company decides to innovate. It mainly outlines two innovation strategies: Disruptive Innovation and Sustaining Innovation. Sustaining Innovation outlines a mainly incremental benefit as it is based on the exploitation of knowledge and skills already widely known and validated within the company with the aim of incrementally improving the performance of existing products. Disruptive Innovation begins with the formation of a new market by converting on-consumers into consumers or by satisfying the customers' bottom-end wants in current markets by offering a product or service that is "good enough."

2.1 History of Blockchain

Many consider blockchain a disruptive technological innovation that will transform our society (The Economist, 2015). But what is so disruptive? Actually, there is no real technological innovation in Bitcoin or Blockchain; all the components were developed long before Satoshi Nakamoto's paper on Bitcoin in 2008. (Aste, Tasca and Di Matteo, 2017).

This concept started in the 1970s with the "Merkle tree," a tree-like structure of concatenated hashes, as the name suggests. These are commonly employed in cryptography to ensure the integrity of digital messages and digital signatures, hence ensuring the security of information. With the introduction of the World Wide Web in 1990, Chaum created the first cryptocurrency for electronic payments: the e-Cash (Chaum, Fiat and Naor, 1990). In 2002, Adam Back introduced the hash cash, a Blockchain-based and Proof-of-Work electronic currency that shares many features with Bitcoin and is considered a reference work by Satoshi Nakamoto (Back, 2002). In late 2008, was published a white paper by a person/group of people called Satoshi Nakamoto, heretofore unknown in which the blockchain-based digital currency Bitcoin was built. Bitcoin's innovation is Bitcoin itself, which thanks to a favorable historical context (financial crisis, technological innovation, and the emergence of new business models) has been able to operate as a market leader in terms of market capitalization and transaction volume (Auctions, Tasca and Di Matteo, 2017).

2.2 Distributed Ledger Technology

The term Blockchain originally referred to the ledger system developed by the Bitcoin protocol, but today it is used to refer to any type of DLT (Distributed Ledger Technology). Distributed ledger technologies are defined as "computer technologies and protocols utilizing a shared, distributed, replicable, simultaneously accessible, architecturally decentralized ledger on a cryptographic basis, so as to permit recording, validation, updating, and storage of data both in the clear and additionally cryptographically protected and verifiable by each participant".

Blockchain is based on the goal of creating a system that does not require an external controller, i.e. a third party, but evolves in a decentralized manner to enable a direct transaction between the parties involved. (Sultan, Ruhi and Lakhani, 2018) Therefore, we can describe blockchain as a distributed and decentralized database containing cryptographically linked sequential blocks. This database stores all transactions that have occurred and shared between portions of the system. It is distributed in that its ledger is public, verifiable and simultaneously present on several computers, and it is decentralized in that the network would continue to function even if one node of the blockchain failed. Given the centralization, there is no single point of failure that hostile actors can exploit to destroy the system (Sultan, Ruhi and Lakhani, 2018). The network types are a centralized network, a decentralized and distributed network.

Every transaction that takes place on the Blockchain is recorded in a public ledger, a register that allows for verification of ownership and transfer of ownership. This ledger is open-source, *i.e.* it is accessible to everyone and can be modified by downloading the appropriate software onto one's own computer. Every computer in the system, or "node," stores an identical copy of the entire ledger, which means that there is no official copy of this database and that every node has the same reliability. One potential problem is duplicate spending, i.e. the risk of spending identical virtual goods twice before one of them has been confirmed. One of these transactions will be confirmed and recorded when it arrives on the network. The consensus system was developed specifically to address this problem, i.e. to get the whole system to agree on which transaction is valid. In reality, the nodes areal fighting for a prize, which is acquired by completing a mathematical challenge often known asProof Of Work (Sultan, Ruhiand Lakhani, 2018).

2.3 The structure of the blockchain, the organization of transactionsand blocks

"The blockchain is a string of blocks that, like a traditional public ledger, contains a complete list of transaction records" (Lai, Chuen, Lee, 2018).
The blockchain is a string of blocks that contains a record of all transactions in a public ledger. Literally, a blockchain is a network of blocks providing information and each link in the chain consists of three parts. The first element is the data included

within the block, the type of information contained in block varies according to the type of blockchain. Here, for instance, the Bitcoin blockchain maintains the specifics of each Bitcoin transaction, including the sender, recipient, and the amount of transferred. The second component is the so-called hash, a string of numbers and letters that uniquely identifies a block and its contents, a form of content that is always distinct, like a fingerprint. Every time a new block is created, a new hash is calculated, unique and specific to that block, and if the block changes, the hash will likewise change. The third element in each block is the hash of the preceding block, and the presence of this hash within each block is what determines its validity. This way of how is build the chain is what makes blockchain so safe. In contrast, the first block seems a bit strange, since it cannot refer to any preceding block, it is referred to as the genesis block. More specifically, the blocks are made up of:

- *Block Header*: representing the block header has some of the above elements such as the hash ofthe previous block, the block number,its size and the nounce value.

- *Block Data*: has a list of the recorded transaction and events associated with the block; other data may also be present (Yaga, 2019).

Hash refers to a string of letters and numbers generated by a hashfunction, which is a mathematical technique

that can transform a string with a variable number of characters into a second string with a fixed number of characters. Even a small change to the initial string can produce a completely different hash (Drescher, 2017). To create the Merkle Tree, one starts with the underlying transactions, labelled A, B, C and D, and generates the hash values of the individual transactions. The hash values are then paired until a single hash reference is obtained, also informally referred to as "the Merkle tree's origin"(Bahga and Madisetti, 2016). Because of this structure, it is no longer possible to modify or remove the contents of individual blocks, since the modification of one block would require the modification of all previous blocks. If we wanted to define the transactions that take place on a blockchain, we could say that they represent an exchange of goods governed by protocol rules; these rules are operationalized by scripting languages and are used even for extremely complicated transactions (Sultan, Ruhi and Lakhani, 2018). As a result, blockchain users send transactions via software simply by connecting to the Internet; each participant has a unique address that allows connection at any time. Transactions are added to the blockchain only after being validated by a publishing node and disseminated to other nodes in the network (Yaga, 2019). It is possible to transfer ownership from one user to another through transactions, but this requires a collection of information, including the data of the sending and receiving users, the date and time of the transaction and the amount to be transferred. Comparing the conventional system to the property transfer procedure, we would have to ask the bank to make the transfer on our behalf under the traditional system.

A wire transfer requires that we provide the bank with allthe essential information to complete the transfer on our behalf. However, the similarity to a bank transferis lost when considering costs. As centralized institutions, banks maintain a standardized fee structure that applies to all consumers. In contrast, for the blockchain that isa decentralized system, it lacks a centralized fee structure, thus each user must indicate in advance the amount he is ready to pay for a transaction. Whoever transfers ownership is also responsible for the cost of the transaction (Drescher, 2017). The adaptability of the blockchain system stems from the fact that its basis is a Peer-to-Peer network composed of nodes with different purposes. One node could validate multiple blocks simultaneously, causing a fork in the blockchain. A Fork is generated when the protocol rules have been updated and not everyone is aware of it. In general, there are two types of Fork: hard and soft.

- The *Hard Fork* is a permanent protocol divergence that network participants may choose to adhere to; if accepted, previously invalid blocks may now be validated.

- The *Soft Fork* could be described as a subset of the previous rules; the new rules are thus a restriction of the old, which does not preclude nodes that have not yet upgraded from participating in the network.

Yaga et al. (2019) illustrate the Soft Fork by assuming that a blockchain reduces the size of its blocks from 1 MB to 0.5 MB. Nodes that upgrade to this new rule will change the block size and continue to operate on the network; non-upgraded nodes will see these blocks as valid because the adjustment made does not violate the previous rules on which they rely. However, if an obsolete node were to generate a block larger than 0.5 MB, upgraded nodes would reject it as invalid, as the new rule prevents this. The Soft Fork will therefore have no effect on the stability and efficiency of the system, as it allows nodes in the network to upgrade gradually (Lin and Liao, 2017).

2.4 The reward mechanism

The development of new blocks requires considerable energy and effort on the part of users, who have to solve an extremely complex problem known as a computational puzzle. This is why they are often offered an incentive or reward, which is a crucial aspect of eliciting positive behavior from participants in the blockchain system. According to Jensen and Meckling (1976) there are two types of incentives: pecuniary ones, which link the agent's observable behavior to a monetary reward, and non-pecuniary ones, which link the agent's observable behavior to a non-monetary reward, such as privileges, visibility or reputation. Depending on the consensus mechanism chosen, the blockchain can use both monetary

and non-monetary incentives. If we wanted to provide an illustration of monetary incentives, we could consider bitcoin: Proof-of-Work (PoW) is deployed and each user who solves the computational challenge is rewarded with bitcoins in proportion to the amount of data in the blockchain that they validated, plus fee. The amount of this fee is determined by the transaction principal and is added specifically to incentivize miners. Indeed, they can choose which transactions to register before others and will naturally prioritize those with the highest fees (Banach, 2019). Ethereum, which uses a consensus methodology called Proof-of-Stake, is an alternative example of a non-monetary incentive (PoS). In this model, all cryptocurrencies are distributed to users and the creation and validation of blocks are assigned through a lottery: the more value one holds, the greater the chances of winning. In this case, the person who creates the block is referred to as a forger; however, the commission they receive will not be in the form of additional coins, but will increase their value in the system, making them more likely to be selected to validate subsequent transactions. Typically, the transaction fees provided by the user constitute the payment for the publication of 14 blocks (Yaga, 2019). This technique has the advantage of being less expensive, but it can undermine the egalitarian and decentralized aspect of a blockchain: individuals who hold more value within the network are more likely to create blocks, earn money on transactions and become richer and richer. Besides this reason, other variants of PoS have been developed and implemented (Narayanan, 2016), like the Delegated Proof of Stake (DPoS). It is used by Cardano and is analogous to the previous consensus

mechanism; it allows a user to 'assign' another node to represent him. Using the language of the stock market, this mechanism allows the formation of groupings of small owners who can compete with those who own a significant number of shares (Yaga, 2019). In other techniques, nodes wishing to participate in the 'lottery' promise a specific amount of the value they own; if they are chosen to establish the blockchain and approve fraudulent transactions, they lose the promised value along with the transaction fees. Instead of relying on incentives, this is based on punishments (Narayanan, 2016). There are further variations on this theme, such as the prohibition to use pledged money again for 30 days. This diminishes the influence of the wealthiest. The 'Byzantine Generals Problem' is well-known research in the field of distributed computing whose techniques are applied in some blockchain (Leslie Lamport, 1982). A parable is used toillustrate the problem of cooperation within systems.Some Byzantine generals are about to launch an assaulton an enemy city. They are at several critical points and can only coordinate the crucial assault through messengers, due to their geographical separation.However, among these messengers are traitors who transmit communications that contradict the army's strategy. Despite the probability of defection, this challenge represents an opportunity to execute the attack successfully. The term for this phenomenon is decentralized consensus. 15 The incoming communication could be coordinated, presenting only one of two possibilities (attack or retreat), or it could be uncoordinated, presenting both alternatives (attack andretreat). Getting a consensus on a distributed networkin which some nodes may be faulty or corrupt is very similar to the problem faced

by distributed computingsystems. Nakamoto attempts to propose a solution to the Byzantine generals' dilemma by emphasizing the needto coordinate the parties. This implies that the attackmust be synchronized and that once the timing of the attack is determined, it will be valid for everyone. This can be achieved precisely through the evidence ofthe work (Narayanan, 2016). The blockchain protocol must monitor the conduct of participants. Failure to do sowill result in the inability to validate the transaction or the removal of anonymity. This could bea viable alternative to incentives: instead of rewarding good behavior, we punish bad behavior, allowing the blockchain to also combat external threats(Banach, 2019).

2.5 Cryptography used by blockchain

Cryptography and decryption are often mentioned when discussing data protection through encryption. “Encryption is the digital equivalent of 'closing a lock', while decryption is the digital equivalent of 'opening a lock’” (Drescher, 2017). Encrypted data may appear as a jumble of meaningless characters and numbers to those who do not know how to decipher it; a key is required to understand it. The process begins with the collection of some data, continues with the encryption of the original data using a cryptographic key in order to produce the cypher text, continues with the transfer or storage of the cypher text, and finally concludes with the decryption of the cypher text using the same cryptographic key in order to retrieve the original data. If a person attempts to decrypt the

cipher text with the wrong key, the resulting numbers and letters would be unintelligible (Drescher, 2017). For many years, encryption technologies with the same key have been used to encrypt and decrypt data. Therefore, the person who encrypted the data could use the same key to decrypt it. The term for this type of encryption was symmetric encryption. On the other hand, it has been demonstrated that it is not a wise decision to encrypt and decrypt information using the same key. In response to this need, asymmetric cryptography was developed. Asymmetric cryptography makes use of two keys that are complimentary to one another; one key is used for encryption, and the other key is used for decryption. The black letter text in an asymmetric encryption can only be decoded by using the white key, and vice versa. The same key cannot be used to encrypt and decrypt the original text (Drescher, 2017). These keys are typically referred to as the private key and the public key. The public key is given out to absolutely everyone, regardless of whether or not they can be trusted. On the other hand, the private key is maintained in a secure location. The information is sent from the public key, which is responsible for encrypting the text, to the private key, which is responsible for decrypting the text. These are the two primary ways that the key pair can be used. Drescher compares this use of the two keys to a mailbox, in which anyone can deposit mail but only the owner can receive it. Therefore, anyone with the public key can encrypt a message, but only the owner of the associated private key can decrypt it. The information passes from the private key, which encrypts the text, to the public key, which decrypts it. In this case, however, Drescher compares this use of keys to a public noticeboard where

only the owner of the private key can post messages that can be read by anyone with the public key. This approach helps prove that the message has been encrypted. Using asymmetric cryptography, the blockchain employs the public-to-private flow to identify users and conduct transactions or transfers between them, and theprivate-to-public flow to authorize transactions. Theuser who intends to transfer something generates the cipher text with his private key and all other nodes canverify his approval of the transfer with his public key. This method is known as Digital Signature or digital signature and is the equivalent of the traditional signature: the encrypted message is its owndigital signature (Sultan, 2018). The person who receives this encrypted message will figure out the message's hash value and decrypt it using the sender'spublic key to get the real hash value. If the two hashvalues are the same, the person receiving the messagewill think that it hasn't been changed and that it really came from the user whose public key it has. Asalready mentioned, there is no central authority thatstores all user-specific private information. Transactions that are included in the blockchain will always preserve their level of anonymity thanks to thistechnology. However, it does ensure that any user can interact with the network with an address that was obtained at random. This does not guarantee perfect anonymity. Additionally, a user can generate many addresses in order to hide their identity. Because he started using the alias Satoshi Nakamoto, it is impossible for us to determine the true identity of theperson who created Bitcoin. (Zheng et al., 2018).

2.6 Other consensus processes

In addition to environmental issues, the blockchain community is exploring alternative consensus techniques for reasons such as scalability. Any alternative consensus method must be associated with a scarce resource that is both attractive to a large group of nodes (to ensure system security and avoid Sybil attacks) and significantly more energy efficient than Proof-of-Work. The Proof-of-Stake (PoS) is the most promising alternative, where the resource is not computational power as is the case with Proof-of-Work (PoW), but capital (or participation), which is demonstrated by the ownership of cryptocurrenciesnative to the respective blockchain (e.g. ETH for Ethereum). In this way it deletes the concept of miners,instead they can deposit an amount of underlying cryptocurrency to become validators. The likelihood of selecting the subsequent validator is related to the amount of the deposit and is determined by a method that uses pseudorandom numbers (Sedlmeir et al. 2020b). Thetotal security of the system here is also guaranteed notonly by the reward, as is also the case in PoW mechanisms (where one receives a reward plus a fee, representingexpected annual returns of up to 18% of the invested capital), but also by the fact that a successful Sybilattack would require more than half of the invested money (which is highly implausible). Furthermore, as in PoW, the validators control each other in a certainway: if one of them is not accepted, it incurs the slashing mechanism, i.e. it loses part of the reward received and can also be removed from the mechanism. Inaddition, Proof-of-Stake could increase the scalability

of Ethereum (or the "x" underlying cryptocurrency) through a process known as *sharding*, which splits the database into many parts called shards, while preserving the integrity of the entire database (Luu et al. 2016). Between the cryptocurrencies there are some that already use the PoS consensus mechanism, such as EOS, Tezos, and TRON, which are among the 20 largest cryptocurrencies by market capitalization (Sedlmeir et al. 2020b). PoS is many orders of magnitude more efficient than PoW because it eliminates energy-intensive cryptographic competition. There are other consensus paradigms besides PoW and PoS, but almost all of them can only be used in "authorized" blockchain.

2.7 Permission and Permissionless Chains

Having explained how it works, we must point out that there are 3different blockchain systems:

1. *Public Blockchain*: decentralization is its main feature, so it does not have a single owner, and is visible to anyone; Each node is able to participate in the consensus mechanism, and all transactions are visible to the public. As a result of the enormous number of nodes, however, the propagation of transactions and blocks is slow. To try to keep the security of the network safe, therefore, the 22 restrictions of the public blockchain may be too strict.

2. *Private Blockchain*: unlike the public it is totally centralized. In this case the nodes will be limited and not everyone will be able to participate in this blockchain as there is strict authority management over data access. However, having fewer validators may be more efficient than the previous system.

3. *Consortium Blockchain*: this type of system is partially centralized; the node with authority can be selected in advance and typically has business-to-business partnerships. Few nodes are accountable for the integrity of the blocks, and one must be authorized to participate in the consensus procedure. The consortium can determine whether or not the data collected is accessible to the public.

3. Blockchain Developments

3.1 Practical application of the blockchain

Numerous applications, financial and otherwise, make frequent use of blockchain technology. The main applications of the technology are the IoT (Internet of Things), finance sector, security and privacy, public and social service, and reputation systems.

In the financial services the introduction of the blockchain, with Bitcoin, "has the capacity to disrupt the global banking industry"(Peters et al.). There are numerous applications for blockchain technology, including the clearing and settlement of financial assets (Peters and Panayi, 2015). Furthermore, Morini (2016) has shown that there are instances where blockchain successfully reduces the costs and risks associated with the collateralization of financial derivatives:

- Organizational transformation blockchain can facilitate business transformation for traditional organizations. For example, blockchain and cryptocurrency technologies could help postal operators (POs) expand their work. Given their strong retail presence, each PO could issue its own postal currency, which would quickly gain ground. In this way they could expand their offering for both new financial and non-financial services (Jaang et al., 2016)

- Risk management blockchain can play an impactful role in FinTech, improving its performance. It can be used to assess investment risk (Pilkington, 2016).

In the following ways, blockchain technology has the capacity to improve the IoT industry:

- In the world of e-commerce, Distributed Autonomous Corporations (DACs) are decentralized entities that enable the use of blockchain and smart contracts to produce smart properties (Zhang and Wen, 2015).

- In the IoT world, there are several projects to protect discretion and security by exploiting blockchain technology. For example, IBM presented a security project, 'the Anonymous Decentralized Peer-to-Peer Telemetry (ADEPT) proof of concept'. This system uses blockchain to build a network of devices that can autonomously identify operational errors and consequently retrieve software updates (Panikkar, 2015).

For the public and social sector:

- *Property Registration*. A typical application of blockchain for the public sector is the land registry, where it is possible to record all changes or cadastral transitions that occur on a piece of land.

- *Energy Savings*. Through mining it is also possible to demolish marginal production costs for renewable energy sources (we will discuss this in the section).

- *Education*. In online education, if we consider the process of learning and teaching as a currency. Teachers could package and insert blocks into the system and learning outcomes could be seen as coins (Devine, 2015).

- *Freedom of speech*. The Domain Name System (DNS) and identities can be protected using blockchain technology.

- *Other public uses*. The technology can help speed up the transition from paper to digital for all those administrative documents such as patents, income tax, marriage registration, etc.

The reputation system is a unique application of blockchain technology. Reputation is a significant indicator of how much a community trusts an individual. In such a system, a person's reputation can be determined based on their previous activities and interactions with society. What blockchain can do to help this system is to reduce instances of falsification of reputation records. The most frequent applications are:

- *Academic environment*. Academic environments attach great importance to reputation. A

company could provide its employees with reputation records; since all transactions are recorded in a blockchain system, any alteration of reputation can be immediately identified.

- *Online community*. In a virtual community, the ability to judge a member's reputation is crucial

The third aspect where blockchain technology can be used is security and privacy. To be more specific:

- *Improving security*. A central server collects, and updates viral patterns used by several anti-malware programmers. Nonetheless, these centralized systems are vulnerable to malicious attacks. Utilizing blockchain technology can enhance the security of decentralized networks. Blockchain can enhance this, hence enhancing the system's dependability and security (Axon, 2015).

- *Privacy protection*. It is well known by now how many mobile services and social networks capture a huge amount of personal data. The blockchain technology could help guarantee ownership of user data, making it more secure from hacker attacks with a decentralized system.

3.2 Cryptocurrencies and Bitcoin

Bitcoin, created in 2009, is the name of both the electronic payment system and the virtual currency used within it. In Bitcoin the capital letter 'B' refers to the technology and network, while the lowercase letter 'b' refers to the currency itself. Therefore, we can say that bitcoin is a currency rather than a payment mechanism. The bitcoin system uses a peer-to-peer (P2P) network, which has no hierarchy. It is a component of client/server systems where each node can act as a client or server depending on the situation. These nodes can be represented by a computer, a smartphone, or any other device capable of running the program. Consequently, Bitcoin does not have a physical medium: currencies can be stored in special wallets installed on one's electronic devices through the installation of software, or in online wallets managed by some portals that provide this service. (Gervais, 2014) This system mainly uses three factors: blockchain technology, cryptography and the mining method to generate new currency and validate transactions. Double spending, i.e. the prospect of the same currency being spent multiple times, is one of the main vulnerabilities digital currencies are subject to. Therefore, each transaction must be examined and validated before it is completed (Karame, 2012). Transactions are validated by network users, who contribute the computing capacity of their machines. Miners are network users who collect and organize transactions into blocks. Each time a miner verifies a block, it is transmitted to the network to be added to the blockchain; in return, the miner receives a certain amount of newly issued bitcoins. The blockchain thus performs similar functions

to an online ledger, recording all transactions and network users. The amount of bitcoin that miners receive for block validation is determined by the protocol and is halved every four years to prevent circulation from exceeding 21 million bitcoins. Proof-of-Work is the cryptographic technique used to force miners to deal with the computational problem of transaction verification (PoW). It turns block validation into a lottery in which the probability of winning increases as the processing capacity increases (Guttmann, 2014). It should also be noted that the software on which the Bitcoin system is based is an open-source software, which is not protected by copyright and in which all participants can modify the system, thus contributing to its evolution and refinement (Guttmann, 2014). Bitcoin, the world's first virtual currency, was created in 2009 by combining a number of existing technologies. Over the past eleven years, it hasexperienced many ups and downs, gained popularity but still raising numerous questions. In order to properlyunderstand its causes, we must first examine its historical origins, before moving on to more recent times.

3.2.1 History of Bitcoin

The bitcoin system represents the realization of the Cyberpunk ideology that emerged in the late 1980s. David Chaum and Wei Daiwere the main proponents of this movement; they believed that computer technology and cryptography were a beneficial tool for individuals to no longer be subject to organizations. In one of his studies, published in 1982, David Chaum introduced the concept of the 'blind signature', a type of digital signature that made it possible to authenticate a

message and determine whether it had been altered during transmission (Subramanian and Chino, 2015). A few years later, in 1989, Chaum launched Digicash Inc, the first company to introduce the e-cash electronic payment system. This method allowed users to store digital currency in their computer's memory and make anonymous and secure purchases on the Internet without going through financial institutions. Digi cash failed in1998 because the market was not yet ready for this change (Guegan and Frunza, 2018). Gold & Silver Inc. was created in 1996 and offered e-gold, a digital currency whose value was determined by the amount of precious metals in the company's reserve. In 2007, the US government accused the company of contributing to money laundering and in 2009, accounts and the ability to transact were restricted (Guegan and Frunza, 2018). Wei Dai proposed a new decentralized payment system in 1998, creating a new currency called b-money; the system theoretically allowed the transfer of value between internet users. It had features comparable to today's Bitcoin system, including the production of money by solving mathematical problems, transactions validated by the digital signature process and anonymity protected by the use of pseudonyms (Dai, 1998). Also in the same year, Nick Szabo created bit-gold, a cryptocurrency even more similar to Bitcoin. For the creation of this currency, a process known as Proof-Of-Work was required to identify a string of bits known as a 'challenge string'. Each string was unique and could only be discovered by the first user to decipher it; users could only move on to the next string after deciphering the previous one (Dupont, 2014). Bitcoin was born from the examination and combination of the above-mentioned projects. Bitcoin initially appeared on 18

August 2008, when 'bitcoin.org' was registered on anonymousspeech.com. The first Bitcoin-related publication appeared on 31 October 2008, in the form of "Bitcoin: A Peer-to-Peer Electronic Cash System", an online document signed by pseudonymous programmer Satoshi Nakamoto. Bitcoin's official debut took place on 3 January 2009, with the production of the Genesis block, a block of 50 bitcoins (Surda, 2014). On 12 January2009, the first official bitcoin transaction took place, between Satoshi Nakamoto and Hal Finney. On 5 October of the same year, the first listing on the New Liberty Standard took place and the bitcoin/dollar exchange rate was assumed to be 1.309, using an equation that included the cost of electricity to run a computer generating bitcoin (Surda, 2014). Following the listing, bitcoin began to gain interest across the global market, giving rise to numerous platforms, such as MtGox in 2010. On 6 November of that year, the exchange rate on MtGox reached half a dollar per bitcoin and the price of bitcoin on the market was $1 million. In 2013, a turning point occurred in relation to the financial crisis in Cyprus. This situation forced the president of Cyprus, the European institutions, and the International Monetary Fund to formulate a EUR 10 billion rescue package. The government's response to this problem included the compulsory withdrawal of funds from bank accounts over 100,000 euro. To save their wealth, Cypriot accountholders exchanged their deposits into Bitcoin. This event caused the value of Bitcoin to increase from $80 to over $260; some economists call this the 'Cyprus effect' (Perugini and Maioli, 2014). Yi, who is responsible for managing Chinese financial flows, stated in a 2013 conference that Chinese residents were free to participate in the

Bitcoin market and that the Central Bank of China was committed to promoting the use of this currency in the long run. Baidu, the BTC trading platform in China, saw its turnover triple in a few days and the price of Bitcoin continued to rise. In January 2014, major Chinese sites, notably Baidu and China Telecom, banned transactions and this led to a significant devaluation of the cryptocurrency (Perugini and Maioli, 2014). (Perugini and Maioli, 2014). The year 2013 will also be remembered for the infamous Silk Road case, which sparked discussions on the illegality of some Bitcoin applications. Silk Road was a dark web platform for the online trade of weapons, narcotics, and other contraband. The portal was unique in that it only accepted payments in cryptocurrency and most sellers left the site within three months of signing up. To remain anonymous, users would register by creating a fake e-mail address and falsifying their IP address with specialized software. In May 2013, a competing site, Atlantis, launched a syder attack against Silk Road, attracting the attention of the FBI. On 2 October 2013, the FBI arrested the site's administrator, Ross Ulbricht15, and the site was subsequently blocked (Van Hout and Bingham, 2014). Following this event, the authorities recognized the need to govern the world of cryptocurrencies because of the enormous destructive potential they demonstrated. On 18 November 2013, the US Senate held a hearing in which the transnational nature of digital currencies and the need for international cooperation to build a unified anti-money laundering framework were emphasized. MtGox's Bitcoin price reached $503, then on 29 November hit an all-time high of $1,206. However, the Chinese government's action caused the Bitcoin price to plummet

to $1,000 within days (Perugini and Maioli, 2014). The year 2014 is known as 'Annus Horribilis' due to the MtGox crisis, problems with other currencies, China's withdrawal, and the arrest of the Silk Road website administrator (O'Hara, 2015). In February 2014, the failure of MtGox eroded confidence in the Bitcoin industry and generated uncertainty about the security of the network. Due to a problem known as 'transaction malleability', MtGox was believed to have lost approximately 750,000 Bitcoins, or $350 million at the time. Between 31 January and 21 February, the value of Bitcoin plummeted from $938 to $111 (Perugini and Maioli, 2014). As of 2016, the Japanese government recognized Bitcoin as functionally equivalent to fiat currencies. In the same year, South Africa's largest market, Bidorbuy, accepted Bitcoins as a payment mechanism. The idea that it is possible to use an alternative currency has spread like wildfire, so much so that the number of Bitcoin ATMs globally reached 771 in September2016. And the price has more than doubled in a year, from $433 on 1 January to $959 on 31 December (Chohan, 2017). A law adopted by the government in April 2017 recognized Bitcoin and other cryptocurrencies as a form of payment in Japan. This law authorized the use of Bitcoins for a range of commercial transactions, including the purchase of goods and services, such as the payment of gas bills. On 14 April 2017, one Bitcoin was valued at $1,177.

On 26 May, the value doubled to $2,244 (Mcginnis, 2019). On 1 August 2017, Bitcoin split into two digital currencies: Bitcoin (Btc) and Bitcoin cash (Bch) (Javarone, 2018). Bitcoin reached $4,900 in September, but in just three months it reached another all-time high, closing 2017 at $20,089 per coin (Taskinsoy,

2019). In January 2018, the price began a decline that led it to lose half its value in one month, dropping to $8,870. The entire year of 2018 is marked by several fluctuations, leading to the loss of $250 billion. Bitcoin ends the year at $3,235, about one fifth of its value in January (Taskinsoy, 2019). Although Bitcoin's share price continued to fluctuate, 2019 was not a particularly spectacular year. On 27 June 2019, it was trading at $13,017 and the S&P 500 indicated a return of around 20 per cent. (Taskinsoy,2019). To date, it should be noted that the cost of creating Bitcoin has increased exponentially, to the point that in some nations it is no longer economical to do so (Cifuentes, 2019).

3.2.2 The technology used by Bitcoin

Bitcoin is a system that employs several technologies, the most important of which are the "Peer-to-Peer network" (p2p) and the "Blockchain". (p2p) is one of the types of distributed systems, which are classified as follows:

- *Client-server systems*: in this system, the server is the sole provider of content and services and the central recording unit. Each client merely requests content or the execution of a service and cannot share its services with other clients (Pourebrahimi, Bertels and Vassiliadis, 2005).

- *Peer-to-Peer (p2p) systems*, on the other hand, are a specific type of distributed

network in which each computer system is referred to as a node.

These nodes are equivalent, autonomous, and interconnected in a highly dynamic manner; they share some of their resources, including processing power, storage, and software and file content. Each node in the network can act either as a client or, as a server for all other nodes in the network, (Pourebrahimi, Bertels and Vassiliadis, 2005). The p2p model can be used in various application fields, including FinTech, payment systems, and document certification and archiving, and distributed computing (Perugini and Maioli, 2014).

The Bitcoin system uses precisely the Peer-to-Peer network; this network is structured in such a way that each participating user communicates transaction information with other users, eliminating the need for an intermediary. This reiterates the decentralized nature of the system, where no central authority such as banks or other intermediaries can intrude (Guttman, 2014).

The blockchain is another technology that allows Bitcoin to function and is probably the most significant innovation brought by Bitcoin; it is the missing link that allows digital currencies to function as distributed peer-to-peer systems (Franco, 2014). All Bitcoin transactions are recorded on the blockchain, making it a truly distributed system. To be included in the blockchain, transactions must be compiled into data structures known as blocks. Whenevera block is added to the blockchain, the transactions it contains

are considered authentic. The process of adding a block to the blockchain is known as mining andis a distributed operation that can be performed by anymember of the Bitcoin network using specialized software and hardware (Delgado-Segura, 2018). The blocks follow a chronological order and are connectedby cryptography; the use of cryptography protects dataand also serves to validate transactions, process payments and regulate the supply of Bitcoins. In particular, Bitcoin uses asymmetric cryptography, whichalways employs two keys: a public and a private one (Badevand Chen, 2014). The anonymity of each user's identity is guaranteed by the fact that they are ableto communicate with the network through a uniqueaddress, known as the Bitcoin address. Digital signatures, consisting of a public and a private key,are used to control the ability to transfer payments through Bitcoin addresses. Specifically, each Bitcoin address has a unique public identifier, which corresponds to the public key and grants authority over the Bitcoins found at this address (Badev and Chen, 2014).

3.2.3 Mining e Proof of Work

As already mentioned, in Bitcoin there is no central authority to ensure trust between parties, so a specific system is needed to confirm transactions: until a transaction is confirmed, it remain spending and can be tampered with; however, once a transaction is confirmed, it cannot be altered and becomes part of the Blockchain (O'Dwyer and Malone, 2014). This problem was solved by Satoshi Nakamoto by combining Mining with Proof-of-Work (PoW). Members of the Bitcoin community

who verify transactions by solving increasingly complicated mathematical puzzles are known as miners. New blocks can be inserted into the blockchain by confirming transactions. This verification procedure causes a competition among the users of the system: whoever solves the computational puzzle the fastest wins the competition (Wu, Pandey and Dba, 2014). When a transaction is successfully validated, a new block is added to the blockchain, and the miner who solves it first receives two prizes: a predetermined number of newly minted Bitcoins and a transaction fee determined by the user who requested the verification (Taylor, 2017). The puzzle that miners attempt to solve is a cryptographic proof function that requires significant time and processing power to solve; a certain amount of calculation must be performed. The difficulty of the puzzle determines the threshold, which is reset every 2016 blocks according to a certain algorithm. Thus, a new block is introduced to the network approximately every 10 minutes. If the average addition time of the previous 2016 blocks falls below 10 minutes, the subsequent 2016 blocks become more difficult to solve. In practice, the difficulty is changed approximately every fortnight (Ma, Gans andTourky, 2018). Miners, in order to increase their chances of being the first to answer this riddle, must strive to increase their processing power. Once a miner believes they have solved the riddle, only one calculation is required to determine whether or not it is correct. Therefore, the work required to validate a block is expensive, while validating its accuracy is much cheaper. As indicated above, after the riddle is solved, newly minted Bitcoins are issued to the miner, but the rate at which this happens decreases over time. In fact, theincentive

for Bitcoins is set to halve every 210,000 blocks until 21 million Bitcoins are exhausted. When allthe Bitcoins have been generated, miners will only be compensated with transaction fees. (Ma, Gans and Tourky, 2018). In general, mining involves solving a Proof-of-Work problem involving a hashcash-type cryptographic technique that requires a certain amount of processing time (Pow). The hashcash is a cost function that describes the amount of work required tosolve a puzzle; it also specifies the number of calculations a miner must perform before discovering the solution. The function accepts an arbitrary-lengthinput and converts it to a fixed-length output calleda hash. The most important component of this functionis that it cannot be inverted to avoid the problem ofdouble spending, which is difficult and expensive to calculate. This function is constructed in such a way that the motivation to verify transactions on thenetwork is greater than the incentive to attack the network. Specifically, Bitcoin uses the SHA-256 function, which produces a 256-bit result consisting of a string of numbers preceded by K zeros. The string of zeros symbolizes the proof of difficulty of the workand the amount of calculation required to solve the puzzle. For each calculation, the cost function outputs a random value between 0 and 256 bits. When a miner reaches an output preceded by K zeros, the proof has been solved. On average,2,000 calculations are requiredto locate an output preceded by Kzeros (Ma, Gans and Tourky, 2018). This verification task is generally rather expensive, especially in terms of energy. In 2016, Aste predicted that about one billion watts persecond (1GW/sec) are consumed to produce a valid Proof-of-Work Bitcoin. It should be noted that there are twomining techniques: -

Solo Mining: when the mining operation is carried out independently by each networkparticipant. In this case, the miner who successfullyverifies a complete block receives the reward in Bitcoin plus the transaction fee. This action becomes more and more expensive as time passes, decreasing thepossibility of a single user solving the PoW alone. Theresult is that users no longer have a guaranteed income (Svensson, 2018). - Pool Mining: is a mechanism used in cryptocurrencies to increase the stability of Bitcoin mining and stabilize miners' earnings. Asindicated above, the increasing difficulty of the procedure has led to unstable incomes for individual miners. In order to increase the likelihood of resolvinga new block, the majority of miners decided to join mining pools and pool their computing capabilities. Once a block is recovered from the mining pool, the administrator splits the reward proportionately amongst participants (Zhu, 2018).

3.2.4 Characteristics and comparison between Bitcoin and fiat coin

According to the Fiat Theory of Money, money is a product of the state or another sovereign power. "Money is a product of law," Knapp states in his 1924 book The State Theory of Money. "The spirit of money is not in the material of the pieces, but in the legal laws governing their use." Fiat money refers to any legal tender established and issued by a central authority, which is accepted in exchange for goods and services due to people's trust in that authority; therefore, it can be said that the factor on which fiat money is based is trust. Bitcoin, on the other hand, is a virtual currency that is not managed by a central authority, but rather by all participants in the system (Lo and

Wang, 2014).

Among the main properties of Bitcoin, we can mention:

- *Decentralized nature*: as mentioned above, Bitcoin is not managed by a central authority and participants appreciate the fact that transactions do not involve third parties; this implies that no financial institution is involved. Since it is predetermined by the protocol, decentralization ensures that no party can increase or decrease the amount of currency in circulation (Sas and Khairuddin, 2017).

- *Low-cost transactions*: Since transactions do not have to go through intermediaries, approval costs are significantly lower than conventional banking transactions. In fact, a Bitcoin transaction costs about EUR 0.10 (Sas and Khairuddin,2017). With the use of Bitcoin, one can move one's money around the world as quickly and easily as sending an SMS: settlement is instantaneous. In comparison, banktransactions take at least three working days to settle (Sas and Khairuddin, 2017).

- *Transparent transactions*: because the blockchain ledger is public, every user can see every Bitcoin transaction, from the first to the last (Sas and Khairuddin, 2017).

- *No inflation*: we know that the maximum number of Bitcoins that can be issued is asymptotically close to 21 million. Bitcoin

thus arises as a currency that cannot be subject to inflation because it has a maximum issuance limit, but it is also a deflationary currency because the supply will tend todecrease and the price to rise over the next 36 years (Weber,2016).

- *Use of pseudonyms*: To participate in the network, it is sufficient to register with an IP address and a pseudonym; when users communicate, only their pseudonym will be visible. Therefore, participants adopt pseudonyms to safeguard their anonymity and identity (Fanti and Viswanath, 2017).

Bitcoin uses the same algorithms as online banks, the only difference being the disclosure of information about users; all information about transactions in the Bitcoin network is shared, but there is no information about the recipient or sender of the cryptocurrency (Ivashchenko, 2016).

3.3 Smart Contracts

In addition to recording the date/time and transaction details, blockchain ledgers can have transactions executed automatically when certain conditions are met, offering a guarantee of execution. A smart contract is a "computerized transaction protocol that executes the terms of a contract", in which the terms of an agreement are written in the form of code recorded in ablockchain, which reads both the agreed-upon provisions and the conditions where the agreed-upon circumstances are to occur and acts automatically when the actual

situations meet the agreed-upon ones.The suggestions for their implementation concern the financial industry, as well as inheritances, where asset distribution is automatically activatedfollowing the death registration, Big Data, and Data Science. The configuration of smart contracts is quitecostly in terms of both energy and expenditure. This makes them more appropriate for repeat agreements rather than one-time contracts; also, they are not appropriate for situations that are prone to significant change during the contractual term. They are most effective when the conditions, and clauses' outcomes are all of a digital nature that can be automated. Unlike traditional contracts, which in some situations allow for contract modification or cancellation with repercussions, smart contracts can only be updated or cancelled in line with the terms specified in the code. Thus, if payment in a smart contract is automated, nothing needs to be changed because the transaction is carried out automatically. Obviously, since the code is considered law, all errorsbecome part of the contract and, by definition, are not outside the 'law.' This relationship between law andsmart contracts has given rise to some speculation talksabout the future of particular career positions, suchas lawyers or notaries. The majority of Smart Contractsacknowledge that they will improve a variety of areas,but they are not expected to replace traditional lawyers or notaries. Smart contract blockchain contracts are significantly more complicated and may necessitate greater power. This will result in higher mining expenses, as well as potential security issues.As a result, security issues may arise. In the contextof applying regular legal procedures to smart contracts, governments will have

to take on newobligations to regulate this new topic. A key role will be given to programmers, who will make judgmentson practical implementations, and as a result, they will be given a lot of power. As a result, they will face increased legal liability. This sector's evolutionwill present new issues to manage in terms of dispute resolution of conflicts, the enforcement of contractualprovisions, or simply because they may be deficient inflexibility and unable to adapt to changing conditions.Because of this, traditional legislation may need to be amended to accommodate for smart contracts' automatedand deterministic character.

3.4 NFTs and other application domains

It is possible to employ Smart Contracts in order to certify ownership of rare digital or physical assets, in addition to creating scarcity for a variety of different forms of digital assets (Yasar 2021). NFTs, or Non-Fungible Tokens, are a sort of smart contract that establishes and certifies ownership of a digital or physical asset that often lives outside of the blockchain. These assets can be anything from software to real- world property (even if it is a digital asset). Smart contracts and non-working tokens offer entirely new applications for blockchain, beyond the cryptocurrencies for which the technology was originally created. This section reviews some of the most well-known uses of blockchain as well as the most promising areas for the future. However, we try to justify why we think each application area is important and worth including in this section.

Nearly any sort of digital content can be claimed, transferred, and verified using NFTs (Non-Fungible

Tokens). Digital art has been the most successful NFT project yet. Crypto art is another name for digital art (Romeo 2021; Campbell and Whitaker 2021). Unlike traditional art forms and collectibles, digital art and other valuable artefacts can be reproduced, disseminated, and used indefinitely without deteriorating in value. NFTs provide something unique and unrivalled: confirmation of ownership of a specific work of art (Clark 2021).

Cryptocurrencies, and Bitcoin in particular, have been shown to act as a hedge against market volatility (Brière, Oosterlinck and Szafarz 2015; Bouri et al. 2017). At the time of writing, NFTs have only been around for a few years, and the extraordinary discoveries of Bitcoin and other digital collectibles are less than a year old (June 2021). Therefore, academic research on the economic characteristics of NFTs has only just begun. However, as the conclusion in section 4.1 shows, this is still the case. It can be assumed that the limited number of functions NFTs allow has contributed to their recent rise in popularity. However, cryptocurrencies (and digital assets in general) have significant drawbacks. In the recent flurry of investment in crypto art, the quality of that art may not have been properly considered. Specialists in the field of art think that "the cultural value of art is being lost." When you buy a work of art, you don't click "buy", you fall in love with it. It's a transaction based on a different kind of relationship (Botz 2018). With the advent of crypto art, shared ownership of otherwise expensive artworks could significantly boost the art market. According to (Sherman 2021), all transactions involving the NFT, and

the underlying asset are also stored in the blockchain. For example, when selling art, it can symbolize the origin of the object all the way back to its creator. An integral part of the proof of ownership is the immutability and verifiability of the blockchain. A verifiable blockchain for ownership can also simplify the problem of authenticity to i) the initialassessment by experts and ii) the preservation of the artwork. If these two services are provided by a certified bank, the level of trustworthiness will certainly, be higher than with anonymous account holders. If blockchain on the one hand solves the problem of traceability and transparency, on the otherhand it has to solve the problem of linking crypto artwith real assets. However, the tokenization of valuablephysical assets for the purpose of collective ownershipseems to be a viable option.

4. Focus on Finance and Regulations

4.1 Application of the DLT in the financial markets

With the advent of digitization and dematerialization of securities, financial markets have to handle an increasing volume of trades and transactions, requiring Central Counterparties (CCPs) and Clearing Houses to monitor a large number of contracts (CCHs). In the context of exchange-traded and over the counter (OTC) derivative contracts, markets must also ensure their execution through the transfer of collateral aimed at limiting credit risk (i.e. the risk that the borrower will be unable to meet its obligations to pay interest and repay principal). CCPs perform this function by intervening in the exchange of securities, interposing themselves between the two counterparties and assuming their credit risk; this entails significant transaction costs for investors, who may be discouraged from buying and selling in this market. To protect trading and exchanges from potential threats to central counterparties, such as the emergence of systemic risk or the insolvency of one or more of its members, a platform known as Distributed Ledger Technology (DLT) has been developed. DLT is able to take over the tasks of central counterparties and replace them within the financial markets, using blockchain technology that can provide security and anonymity to investors. Through the construction of a ledger, this technology enables the creation of a historical memory to govern and manage trades and transactions. In Distributed Ledger technology, the ledger can be updated,

monitored, regulated, and coordinated not only centrally, but also by all participants in that platform; in this way, each member is aware of the transactions that have taken place while maintaining anonymity.

To safeguard their investors, financial markets must be able to develop a secure trading environment and adhere to numerous requirements regarding open information, confidentiality of trading strategies and investor tracking. Distributed Ledger Technology has three primary objectives:

1. secrecy of information
2. data integrity
3. the security of users

The confidentiality of information is guaranteed by the fact that, in a DLT characterized by a private network, only network participants can access the information in the shared database; therefore, other parties cannot access it. Furthermore, a large number of companies are developing different programs that can createdifferent layers within the same network to provide access to different types of information, thus limitingthe number of actors that have access to strategic information that can influence investors' market decisions. In this way, participants can function by adhering to different investment plans and ensuring the same level of competitiveness in the financial markets.

Data integrity, on the other hand, is maintained

through database updates made after the confirmation of each transaction. Once these changes are implemented, the data become immutable over time and cannot be modified without the approval of all network participants and after targeted tests to ensure the legality of such changes. Finally, user security is ensured by the application of cryptographictechniques, such as the use of digital signatures, whichcan ensure adequate anonymity to the transactions taking place between the various network participantsand protect the information shared from potential external attacks.

One of the characteristics of Distributed Ledger Technology is its ability to guarantee its participants an operating environment with a high level of security and robust resistance to a variety of operational problems, ranging from a potential cyber-attack to the malfunctioning of internal structures. DLT establishes selection criteria for its participants that identify those who are unable to comply with the agreed standards and uses encryption to make shared information inaccessible to unauthorized parties. Distributed Ledger Technology, should it be applied to financial markets such as the Over-The-Counter derivatives market, requires special care during its development; firstly, since it is a fundamental sector of the global economy, it is preferable to use a DLT characterized by a private network to limit access to confidential information shared within the network. Furthermore, although this technology is destined to replace CCPs, its refinement is still at an experimental stage,and it is preferable to initially entrust its managementto a consortium of authorities of various types, such as

commercial banks, which can regulate the access of the various actors, but also ensure adequate trust for investors who choose to operate in the network; in this way, one avoids exposing network participants to high risks that could compromise the integrity of thenetwork itself. Furthermore, in order to strengthen thesecurity of users, when a transaction is finalized, itcan be confirmed not only by the users of thenetwork, but also by external third parties with a highlevel of trust, which can guarantee adequate verification of the conditions that the two counterparties must fulfil. Moreover, many users prefer to obtain payments through the use of real and trusted currencies, suchas the dollar, rather than digital currencies such as Bitcoin; therefore, a concrete involvement of central banks, or their institutions capable of distributing liquidity to the market, would encourage more users to use Distributed Ledger Technology for their daily transactions.

Another important consideration is that the participants in the various transactions operate in countries with different laws; one must therefore try to overcome this limitation by creating a new regulation capable of ensuring that the transactions carried out are as standardized as possible and do not violate the laws in force in the various countries, including through targeted legislative interventions. The introduction of Distributed Ledger Technology in the financial markets would change many features of the current regulatory structure; in particular, with the use of smart contracts, the time required to execute transactions, typically several days, would be drastically reduced. This change would lead to a

significant improvement in operations, as traders would be able to conduct very fast transactions whose effects could be observed almost in real time, but there could be a significant liquidity problem; there could be more frequent requests requiring a change in the infrastructure of many central banks responsible for providing liquidity to the market. In addition, some important current market participants will be rendered obsolete, such as central counterparties that interpose themselves between the various players and intermediaries whose responsibilities would be altered. Distributed Ledger Technology is undoubtedly a very useful technology for coping with the high volume of transactions and exchanges in the market and for speeding up and securing many transactions, including those that are critical to some economies. However, it also requires substantial legal and infrastructural change to ensure the full availability of the transactions it facilitates. DLT has already been applied on an experimental basis on a global scale, with the Monetary Authority of Singapore developing a project for the execution of payments and the exchange of securities and the Bank of Canada developing a project for the settlement of interbank wholesale payments.

4.2 Regulation of the cryptocurrency world

The advent of new technologies, new markets and new entities interfering in these markets makes it necessary to implement new laws to regulate these areas,

or at least to examine the applicability of current laws to them. Until now, there has been considerable confusion about the optimal regulation to be applied to the Bitcoin industry, and this uncertainty has had a number of detrimental effects:

- first, it hinders the flow of institutional funds and investment capital needed for the development of cryptocurrencies;

- second, consumers are typically wary of cryptocurrencies due to their unknown legal status and lack of government recognition or approval.

Therefore, precise and specific rules are needed to address these concerns. Such rules would serve both to safeguard users from the dangers of malicious actions and, more importantly, to ensure that individuals can safely exploit the discoveries of new technologies. (Lim, 2015) Cryptocurrencies, or virtual currencies, are one of the most significant financial innovations. The term 'virtual' indicates that they do not exist in physical form but are created and shared through telematic techniques. As we have seen in the previous paragraphs, cryptocurrencies have adapted some of the concepts of traditional fiat currencies to their environment. For example, cryptocurrencies have replaced traditional wallets with digital wallets called wallets (Consob,2019). Due to constant price volatility, virtual currencies are unable to perform some of the primary functions of traditional fiat currency; for example, they are not legal tender;

therefore, it is at the discretion of individual users to accept them as a form of payment. Moreover, as has been said many times, they are decentralized entities that are not regulated by any central government body, although some nations, such as Venezuela, are trying to use them by attempting to control them (Consob, 2019).

Thousands of cryptocurrencies are currently in circulation, perhaps partly due to the fact that anyone can create one. ICOs, which stand for Initial Coin Offerings, can be used to generate, or simply distribute these virtual currencies. ICOs are the method by which a group of individuals or an individual entrepreneur can raise capital to finance their ideas in exchange for one or more tokens. It is advantageous to obtain funding through ICOs as there is no need for an expensive third-party funder to participate and they are not subject to geographical restrictions (Burns and Moro,2018). The use of blockchain allows ICOs to achieve higher levels of security and transparency, fostering trust within the system. There are three types of tokens that can be issued by an ICO (Burnsand Moro, 2018):

- *utility tokens*: which offer a license to use a software program,

- *security tokens*: which offer the opportunity to earn a share of the company's future revenues,thus acting as collateral,

- *payment tokens*: which act as a medium of exchange for investors.

In general, the release price of the tokens is set arbitrarily by the ICO team. However, once the ICO is concluded, the price will be determined by the supply and demand of investors. However, the ICO team may also initiate a kind of pre-sale or pre-offer in which tokens are sold to major investors at reduced prices before being released to smaller investors (Burns and Moro, 2018). Initial Coin Offerings are comparable to Initial Public Offerings, which represent the first sale of shares to the public. However, these two processes differ significantly: in IPOs, shareholders have voting rights, receive shares in the company, are managed by underwriters and are highly regulated. In ICOs, on the other hand, companies are typically very young or even start-ups; tokens, unlike shares, represent an opportunity to use the company's service in the future and are also self-managed by teams. The main difference is that ICOs are not regulated, as they are structured to avoid specific regulatory requirements (Burns and Moro, 2018). As they are not always able to thoroughly research the project, assessing the potential value of the ICO can be one of the challenges that investors encounter. Investors can try to assess the quality of the team and the white paper, but they can also check the rating provided by numerous websites.

Consob (2019) says that the fact that initial coin offerings (ICOs)are not regulated in a specific way has led to a rapid growth of these practices in the past few years, which has contributed to a surge in the value of major cryptocurrencies such as Bitcoin.

In addition, the sites where cryptocurrencies are sold or bought arealso unregulated, so customers who could suffer huge financial losses have no recourse if problems arise. The risks associated with this lack of regulation include a lack of transparency and, above all, security, which encourages the growth of cybercrime. Due to theuse of pseudonyms, European officials believe that cryptocurrencies can be used for money laundering or,as in years past, for the illegal arms trade. Conversely, investors believe that virtual currenciesoffer several advantages over the current system, suchas faster processing of transactions and lower transaction costs. They believe that the new technologies provided by cryptocurrencies have the potential to change and improve the current economic structure. As this phenomenon affects many countries around the world, each government is trying to establish appropriate legislation. Some are even trying to integrate cryptocurrencies within currently regulated categories, while others are trying to create ad hoc regulation and still others have banned cryptocurrencies altogether (Venettoni and Magnanini, 2018).

Regulation and legalization of cryptocurrencies could improve conditions for users and businesses. This regulation, however, does not have to be uniform in all countries, as a regulation that is effective in one nation may not be so in another. In the UnitedStates, for example, restrictions vary from state to state (Venettoni and Magnanini, 2018). In Australia and Japan, cryptocurrencies are considered property and are regulated by their own set of rules. Undoubtedly,Japan

is the nation where cryptocurrencies are most developed and used. In Canada and South Korea, on the other hand, cryptocurrencies are not considered legal cash, although they can be traded legally. As we haveseen, each jurisdiction has decided to treat the Bitcoinsector differently. It must be recognized that this isa very new and emerging market, and only by trying to understand the technologies used and how they work will it be possible to determine the appropriate regulation. Let us now turn to our own country. Consob is responsible for regulating the financial industry and protecting investors in Italy. It has launched a public enquiry to explain the legal approach to cryptocurrencies and to define permissible and illegal behavior. Consob (2020) defined the financial product category and clarified that it includes investments of a financial nature; to be included in this category, such investments must meet the following criteria: "the use of capital, a promise of return of a financial nature and the assumption of risk associated with the use of capital". Consob has added requirements with the passage of time and the emergence of new financial technologies. In the case of tokens produced through ICOs, they promise future rewards that cannot be classified as monetary gains. In an attempt to define the category of cryptocurrencies, Consob outlined the distinctive characteristics that virtual currencies must have in order to be included. Firstly, they must employ creative technologies that incorporate the rights of the parties that choose to invest in them, such as blockchain; secondly, they must use these innovative technologies for the transferability of tokens and for recording and storing the rights of cryptocurrency users (Villanueva Collao, 2020). Consob says that the

only people who can use these platforms are operators of risk capital collection sites whose work is governed by Consob Regulation No. 18592 of June 26, 2013, also called the Crowdfunding Regulation (Villanueva Collao, 2020). Those who are already authorized to operate crowdfunding platforms may also operate platforms for the offering of cryptocurrencies, provided they have made a prior application to Consob and keep the two activities separate. These entities must deal with cryptocurrency issuers and request from them any information they deem essential for investors to determine whether or not to invest. Consob can then decide the guidelines for the provision of this information, allowing all investors to evaluate the many investment opportunities and select the best one (Villanueva Collao, 2020). Consob (2020) determined, due to the continuous evolution of this market, that it would be impossible to design a regulation because it would risk stifling the continuous improvements of the system. The chosen regime is therefore based on an opt-in mechanism, which allows organizers to choose between using a platform dedicated to the offering of cryptocurrencies, which was previously named, thus guaranteeing a minimum level of regulation, or a platform that does not fall under the latter, which would not offer investors the same level of protection as the former. Consob is responsible for supervising the platforms selected by operators under the Crowdfunding Regulation, as well as the offers made on these platforms. In the event of violations of these rules, operators risk administrative and criminal sanctions, which also involve the issuer of the cryptocurrency,

Exchange mechanisms also fall within the scope of cryptocurrencies. We can distinguish between systems that facilitate the trading of tokens (exchanges), thus facilitating the meeting of supply and demand, and those that only handle the custody or transfer of tokens (wallets). Exchange platforms often also offer wallet services (Villanueva Collao, 2020). Recall that wallets are special systems in which users store not only the keys used to identify themselves on the blockchain, but also their tokens. Exchange systems record every transaction that takes place on the platform and the subsequent transfer of tokens. Currently, the rules and structures are determined directly by the technologies used, which are based on distributed ledgers; however, there is undoubtedly a need for a framework that establishes the parameters for the operation of such systems (Villanueva Collao, 2020). Consob has therefore considered the creation of a label, which consists of the registration of the exchange system with Consob itself, in order to improve the dissemination of ICOs and stimulate greater interest among market participants, such as banks. Consob wouldalso assume that only cryptocurrencies that arepublicly available on one or more exchanges can be traded:

a. "Transparent and non-discriminatory rules and procedures regarding the conduct of trading;

b. effective procedures to ensure that up-to-date information on cryptocurrencies has been published on the system at the time

trading begins;

c. procedures to identify and manage the risks to which the system is exposed;

d. measures necessary to facilitate the efficiency of the system" (Villanueva Collao,2020).

In conclusion, we can state that cryptocurrency regulation is important to ensure the protection of consumers and investors from potential fraud, as well as to ensure the integrity of markets and payment systems in order to increase financial stability (Archeret al. 2018).

4.3 Decentralized Finance (DeFi)

First-generation blockchains, like Bitcoin's, created a shared database of transactions, then second-generation blockchains, like Ethereum, added smart contracts to blockchain technology. So, "decentralized finance" came into being.

Decentralized Finance, or DeFi, is an ecosystem of financial apps, called DApps, that were mostly built on the Ethereum blockchain. More specifically, decentralized finance is a movement that wants to make financial services (like borrowing, lending, and trading) that are open source, decentralized, transparent, available to everyone, and don't need a central authority. Users keep full control of their assets in this decentralized, peer-to-peer ecosystem.

This new ecosystem, which is made up of blockchain, smart contracts, and cryptocurrencies, could change the traditional banking and financial world by replacing middlemen with a system that doesn't need trust, has no borders, is transparent, and is cheap. Also, thanks to DeFi, it can make it easier for people to use financial services, make sure data is safer, make agreements without trust through smart contracts, and offer new financial products.

4.3.1 The main advantages of the DeFi

In traditional finance, banks and other institutions act as middlemen. DeFi applications, on the other hand, do not need these figures. Decentralized digital wallets make it possible for users of DApps to keep full control of their money. Also, these new services could have a high level of data security because they are registered on the blockchain and spread across thousands of nodes.

The DeFi movement also makes it easier for people who are left out of the current financial system to get financial services. In 2018, the Federal Reserve estimated that 55 million people in the US and about 2 billion people around the world did not have a bank account. Another possible benefit of DeFi is that DApps from different blockchains will be able to work together. This will make it possible to create completely new markets, products, and services.

4.3.2 The main applications of the DeFi and its challenges

In this subchapter, we will discuss the main DeFi applications:

- Stable coins are a type of digital currency whose value is tied to the value of a real asset. Many Stable coins are tied to the value of the US dollar, while others are tied to the value of gold or silver. This kind of digital currency is called used to avoid the high volatility that is common in cryptocurrency markets.

- Decentralized markets (DEX): make it possible to exchange different cryptocurrencies, or to buy and sell crypto for fiat currencies. The prices of assets listed on an exchange depend on demand and supply, so each exchange calculates its price based on its trading volumes. This means that the larger an exchange is, the closer the prices will be to the real market price. There are two types of exchanges: centralized and decentralized. Centralized exchanges centralized exchanges (CEXs) act as intermediaries for asset management. Conversely, decentralized exchanges (DEX) are exchange markets that do not rely on a third party to maintain users 'funds. Transactions take place directly between the users' wallets (peer to peer), a feature that mirrors the principles of a blockchain. In DEXs, unlike CEXs, the user is truly the owner of his assets as he is the only one in possession of the access keys to the wallet. Moreover, being a system decentralized onblockchain, the risk of

hacking is very low compared to that of the centralized platforms of CEXs. However, DEX, unlike CEX, can still be difficult to use, have less liquidity and there isno assistance in case of problems.

- Lending: open and decentralized lending are one of the most popular applications within the DeFi ecosystem. These protocols bring numerous advantages over the traditional lending system. For instance, they make cheap access to credit, settlement of the transaction is instantaneous and include the possibility of collateralize digital assets that can be sold to the detriment of the debtor, if the latter does not perform its obligation. It is therefore possible to earn interest by depositing stable coins in liquidity pools. Since these lending services are registered on public blockchain, they reduce thetrust required and offer immutability through cryptography.

- Synthetic assets: DeFi also allows the creation of synthetic assets. These synthetics track the value of the corresponding real-world assets. To replicate the prices of synthetic assets oracles are used that take information from traditional financial platforms traditional financial platforms. This system favors exposure to traditional assets such as currencies, commodities, stock indices, cryptocurrencies and stocks. All this directly on the Ethereum blockchain. Currently, the most widely usedplatform for creating synthetic assets is Synthetix.

It is important to emphasize that, at present, DeFi is at an experimental stage, but is rapidly evolving. In this new industry, computer security is still one of the most substantial threats substantial. For this reason, external (but not institutional) auditing bodies are emerging (Quantstamp, OpenZeppelin and Certora) to certify and audit the functioning and robustness of smart contracts in platforms. Currently, the lack of sufficient regulation discourages traditional insurers from offering protection for this type of digital asset. Moreover, most platforms incentivize the entry of liquidity by using dynamic interest ratem odels that dynamic interest rate models that produce variable rates depending on the level of liquidity within each asset pool. However, incentivizing liquidity does not always mean guaranteeing it. In these early stages, the risk of user error is high, as is often the case with new technologies. DeFi applications transfer the responsibility of intermediaries to the user. This can be a negative aspect, especially for new users. Therefore, the challenge is to make technologically complex products user- friendly. Therefore, for decentralized applications to become a central element in the global financial system, they must provide tangible advantage that incentivizes users to abandon the traditional system. With the passage of time, this emerging sector could develop further to the point of seeming unrecognizable from what it is today. If successful, DeFi will shift the power of large, centralized organizations into the hands of the open-source community and the individual. If all this will create a new financial system will only be seen once the DeFi tools are ready for mainstream adoption.

5. Energy consumption and environmental footprint of the Blockchain

In recent times, the topic of energy consumption and the environmental footprint of blockchain has been at the center of numerous debates. The energy consumptionof a blockchain based on the Proof-of-Work consensus method is essentially due to the work done by miners insolving a cryptographic puzzle. This is a task that canonly be tackled with a brute-force approach i.e. trying all possibilities so that only the pure computing powerof the miners counts. The miner who has to solve the puzzle first coins the block and receives a reward in cryptocurrency. In contrast, the energy consumed to perform transactions when the block is minted is negligible compared to that used by the Proof-of-Work.In other words, minting an empty block consumes almostthe same amount of energy as minting a full block.

Considering the blockchain at a general level, we can say that there are three players involved in energy consumption, respectively in order of the degree of impact:

1. the calculation resulting from the consensus mechanism (specifically PoW if applicable);
2. the storage of the distributed ledger; the communication between the various nodes, which can be triggered by the following events:
    a. messages from the consensus mechanism,

b. the transactions,

c. following the addition of a node, the download of the entire blockchain.

5.1 Energy consumed by the calculation resulting from consensus mechanisms

It is crucial to understand the importance of the PoW mechanism in blockchain technology to measure how much they actually consume. The energy consumption of PoW consents is intrinsic to their purpose of encumbering consensus participation in order to prevent Sybil attacks. Miners voluntarily incur costs in advance in the expectation of a potential future reward. The miner who first manages to solve the complex calculation will receive one-unit of the new mined currency. This is a clever way to ensure the consistency and security of the blockchain as the reward is only distributed if miners behave clearly according to the rules of the blockchain protocol. We can subdivide two types of financial costs:

1. Capital costs, i.e. fixed costs, such as the purchase of specialized hardware to deal with the computational complexity of consensus mechanisms.

2. Operating expenses, i.e. continuous variable costs dominated by the cost of electricity to run the specific hardware.

Importantly, as the price of a cryptocurrency that relies on PoW consensus mining (such as Bitcoin) increases, energy consumption also increases and this can become an environmental problem (de Vries 2018), as happened during the first Bitcoin run in 2017 (Higgins 2017).

5.1.1 Upper limit for energy consumption of the consensus mechanism PoW

The main driver of electricity consumption of a PoW consensus system is the expected profitability of the miners: the latter will continue to mine or continue to increase if it suits them, i.e., as long as the expected profitability is greater than the actual costs. Operating costs are more predictable and are mainly determined by the cost of electricity the increase in the price of Bitcoins with the decrease in electricity costs generally leads to an increase in electricity consumption given the higher profitability and the commitment of more hardware.

The cost variable for each individual miner must, as we have seen before, include both cost items (fixed and variable) and in particular must therefore include the price of electricity required for the calculation:

$$C = \#H * EI_h * PUE * P_E$$

Where:

- C is the miners' costs for a period,
- $\#H$ is the number of hashes the miner performs in that period, and which has no unit of measurement as it is only a number but for completeness, we

measure it in [hashes],

- EI_h is the energy intensity of the hashes and is expressed in [Joules/hashes],
- *PUE* is the "utilization efficiency", which relates the energy consumed by the entire IT structure to the portion of energy used solely for IT operations,
- P_E is the price of electricity expressed in a currency in Joules [USD/Joules].

At this point, since the goal of the hardware is to process as many hashes as possible in the shortest time frame, it is possible to write:

$$C = t * HR * EI_h * PUE * P_E$$

The hash number H was replaced by introducing:

- t the length of the mining process in seconds [s],
- *HR* the hash rate expressed in [hash/s].

We now calculate the gain that is expected by the miners. It will depend on the operations the miner will be able to complete (hashed) compared to the total operations of all miners needed to arrive at the nounce. Moreover, the expected value for the correct nounce is 16N (similarly 2^{4N}), where N denotes the number of initial zeros to be obtained. The expected gain from a miner:

$$E(R) = \frac{t * HR}{2^{4N}} * \#CC * P_{CC}$$

Where:

- $E(R)$ is the expected gain,
- N is the number of initial zeros expected,
- $\#CC$ the number of cryptocurrency units assigned to the miner who first arrives at solving the mathematical problem,
- P_{cc} the price of the cryptocurrency assigned to the minermeasured in [USD].

Looking at the equation we can divide two terms, a fraction, and a multiplication. The former indicates theprobability of the miner solving the puzzle, i.e. the number of total hashes he or she manages to perform before the end of the operation. The second, on the other hand, is the gain the miner expects.

Obviously, as long as it is profitable for the miners to continue operating, they continue to do so, i.e. as long as E(R) is greater than C. This is an abstract system, the miners mine as long as the expected revenue exceeds expenditure, thus keeping the time for mining to reach revenue reasonable.

In response to this need for competitiveness, mining equipment has improved over the past decade, also improving the total energy consumption per calculated hash rate. Initially, miners used conventional CPUs in their PCs, and then with time moved to FPGAs or field-programmable gate arrays and later to ASICs, application- specific integrated circuits with significantly improved performance and efficiencies.

Now writing the equation between costs and gains we have:

$$\cancel{t * HR} * EI_h * PUE * P_E = \frac{\cancel{t * HR}}{2^{4N}} * \#CC * P_{CC}$$

The term $t * HR$ is simplified and considering the other factors as constant, we can derive the energy intensity for a hashing operation:

$$EI_h = \frac{1}{2^{4N} * PUE} * \frac{\#CC * P_{CC}}{P_E}$$

We can see this energy intensity found as threshold, and here are the reasons why:

- it is exactly proportional to the expected return, #CC * P_{cc}, and consequently to the price of the currency used;

- it is inversely proportional to the average price of electricity Pe and also to PUE, i.e. everything that increases the cost of mining. However, it is also inversely proportional to the difficulty of the mathematical problem to be solved.

Using Bitcoin's current statistic (September 2022) would give N = 20, #CC = 6.25, and approximately *PUE = 1.3* (as we can see from the CBECI, the Google's PUE is 1.11 but the PUE for the most data center is 1.8; considering the best-case scenario, where are used optimized facilities to mine the PUE is 1.01. Thus, the number 1.3used comes from a weighted average), P_{cc} = *22,000 USD* (rounded) and P_E = *0.05 USD/kWh*, (as also

used by CBECI, 2022) and representative dividing the previous number by 3.6 million (to convert from USD/kWh to USD/J) gives an energy intensity of EI_h =6.30 * 10-12 J/hash, i.e., EI_h = 0.063 J/GH

By estimating the energy intensity of the PoW process, we can determine an upper bound for the total amount of energy that will be used in a specific amount of time:

$$E = PUE * EI_h * \#H$$

Moving on to power, we may divide both sides of the equation by time to get:

$$P_{PoW} = \frac{2^{4N} * PUE * EI_h}{t}$$

Over a period of time the expected number of hashes is $\#H = 2^{4N}$. Substituting EI_h for the calculation made earlier:

$$P_{PoW} = \frac{2^{4N} * PUE * EI_h}{t} = \frac{2^{4N} * PUE}{t} * \frac{1}{2^{4N} * PUE} * \frac{\#CC * P_{CC}}{t * P_E}$$

Substituting Bitcoin's current data, as we have done previously, and considering that a period t is about 10 minutes, $t = 600s$, we obtain a consumed power of Bitcoin's PoW consensus mechanism of $16.5\ GW$ that we

can convert to E_{PoW} energy of about *145 TWh per year*.

Just as a practical example of what it is explained previously, it is possible to see that increasing the current price of the Bitcoin the energy consumed will increase. If we consider a Bitcoin price of *40,000 USD* and all the other parameters remain the same, we obtain an annual energy consumption, $E_{PoW} = 263\ TWh$.

5.1.2 Energy required for the computational complexity of alternative consensusmechanisms

An alternative to PoW is the secure and less energy-intensive consensus method: proof-of-stake (PoS),where electricity is replaced by cryptocurrency capital (stake) locked into the blockchain protocol. Instead of having to prove that you have done the work,you simply have to prove that you have put a large amountof money into the blockchain protocol without having to calculate complex mathematical problems. The complexity of PoS consensus processing is much more efficient especially for large systems, because it does not depend on the amount of nodes in the entire network. Therefore, in general, the energy consumption for PoS is lower than for PoW consensus mechanisms and also does not increase with the value of the underlying cryptocurrency price or the sizeo f the network.
Many blockchains have been created using this alternative consensus mechanism, *e.g.* Tezo's blockchain. The use of the PoS method greatly reduces the energy consumption and ecological footprint of the blockchain, as confirmed by a thorough report presented by PwC in collaboration with Nomadic Labs. Ethereum, the

second largest blockchain by market value after Bitcoin, is slowly transitioning to the PoS consensus mechanism. The lengthy upgrade process started on 31 December 2020 and is expected to be completed by the end of 2022.
It is not yet clear how alternative consensus algorithms like PoS can replicate the same security guarantees of PoW and with what trade-offs. So far, it has been empirically shown that the PoW approach is more secure even with 100% of the computational power of the network.

5.2 The amount of energy consumed to store the DLT

As we have previously illustrated, blockchains can be conceptualized as distributed ledgers. Each mainstream blockchain implies the replication of the entire chain from the beginning. Estimating the energy consumption of the nodes of a blockchain is not straightforward because they might run on a variety of hardware platforms.

The yearly energy usage of a fully replicated blockchain's storage may be computed as follows:

$$E_{St} = \#Repl_{Av} * BC_{St} * EI_{St}$$

Where:

- E_{St} is the annual energy for storing the blockchain in[kWh/year],
- BC_{St} is the dimension of the stored blockchain in [GB],
- $\#Repl_{Av}$ is the annual average number of replicas

weighed,

- EI_{St} is the average energy intensity of storing one unit (1GB) for one year in [kWh/year*GB].

If we take a blockchain (without permissions) we can determine its size and estimate the number of nodes (and thus also replicas) (Bitnodes 2022). With regard to the average archive energy intensity of a unit, it is necessary to make some assumptions:

1. According to Bitocoin.org, nodes are always on, or rather, it is recommended that they are always on, although the minimum requirement is 6h per day.

2. The nodes can run on PCs, thanks to the presence of Bitcoin software, but more importantly, due to the low requirements of GB required for the RAM and the disk space. Of course, more efficient servers could also be used, but we take this as a conservative assumption that could cause an overestimation, but not by much.

If we consider an average PC power consumption of *30 W* (between the consumption of a normal laptop and an efficient desktop), on*8,760 hours* in a year we get *263 kWh/year*. At this point, all that remains is to calculate the replicas, because when blockchains are stored entirely on dedicated nodes, we can directly use the next equation:

$$E_{St} = \#Repl_{Av} * E_N$$

Where the energy for blockchain storage is calculated directly from the average of the number of replicas and the average energy required by a node on the blockchain (last two terms of the q first multiplied)

For Bitcoin, given a current estimated average of about *14,000 full nodes* (Bitnodes 2022) and the *145 TWh* per node and year calculated above, this would give an annual storage energy of about E_{St} *= 2 GWh/year*; as discussed above, probably an overestimate.

In fact, by modifying the second assumption to state that all nodes are stored in big data centers (DCs), an assumption closer to reality and certainly closer to the future, it is possible to find a hard threshold of a factor almost *100 MW* lower than the maximum limit of *2 GWh* per year, calculated with the alternative storage assumption (Coroamă, 2021).

Until now, we have assumed that the blockchain is entirely replicated at each node participating in the chain, but in reality, for reasons of efficiency and scalability, blockchains can be broken down into 'fragments' (Luu et al.2016). For example, the Ethereum blockchain has multiple shards. In such a blockchain, each node will only store one of the fragments and not the whole chain. It is possible to rewrite the equation in a more general way:

$$E_{St} = \sum_{i=1}^{\#shards} (\#Repl_i * S_i) * EI_{St}$$

Where:

- *#shards* are the number of shards in the blockchain,
- $\#Repl_i$ is the number of nodes replicating the *i-th* shard inthe chain
- S_i is the size of the *i-th* shard.

As can be seen from the equation the implicitassumption present is that the energy intensity of storage is independent of the shards and thus EI_{St} canbe taken out of the summation.
In general, this distinction of shards should not change the results we have found so far by much. Furthermore, a sharded blockchain that aims at scalability will certainly grow faster in size than a non-sharded blockchain. In particular, if we have a growth of nodes, it may be relevant if PCs are used for storage, whereas if DCs are used, the overall size becomes more important.

5.3 The amount of energy required for communication between nodes

In addition to performing the actual calculation, a PoW consensus mechanism broadcasts the appropriate message to the full branch of nodes, hence creating traffic. Coordination messages supply the energy usage information:

$$P_C = \frac{Bl * \#N * (EI_{WAN} + EI_{FAN})}{tt}$$

Where:

- B_1 is the dimension of a given block,
- $\#N$ is the number of nodes on the blockchain involved in the consensus mechanism,
- EI_{WAN} and EI_{FAN} are the energy intensities measured in [kWh/GB]of the wide-area grid and the fixed access grid (Coroamă 2021),
- tt is the average time of the two blocks [s].

The actual figures for Bitcoin are: $B_1 = 1\ MB$ (Bitstamp.net, 2022), $\#N = 14{,}000\ full\ nodes$ (Bitnodes, 2022), $EI_{WAN} = 0.\ 02\ kWh/GB$ and $EI_{FAN} = 0.07\ kWh/GB$ (Coroamă 2021), $tt = 600\ s$ (Sedlmeir et al. 2020a). Employing these numbers in the fraction counter of equation yields an estimated total communication energy consumption of only
$0.09\ kWh/block$ and splitting this average consumption by time yields the average energy usage due to Bitcoin's communication complexity, which is $P_C = 0.562\ kW$, less than a boiler on somewherein the world. Since a year includes $8760\ hours$, the overall annualenergy consumption of blockchain communications is just about $E_C = 5\ MWh$.

6. Critical discussion on the paradigm between energy consumption and Bitcoin

6.1 The primary elements influencing blockchain and Bitcoin energy demand in comparison

In light of what was seen in the previous section (5), it can be inferred that not only the energy required for coordination messages between nodes can be ignored, but also the energy consumed by the storage of the global blockchain. Thus, from both an environmental and political perspective, the only technologicalcomponent that needs to be analyzed in more detail isthe PoW consensus mechanism.

The Cambridge Bitcoin Electricity Consumption Index (CBECI) is a project created at the Cambridge Center for Alternative Finance, an independent research institute based at Judge Business School at the University of Cambridge. According to the CBECI, today the Bitcoin blockchain uses 10.78 gigawatts of electricity which corresponds to a total annual electricity consumption of 94.5 terawatt-hours, the figure is an annualized measure that assumes continuous high energy use over a period of one year. This is 0.59% of the world's total annual electricity consumption. Let us put these figures in perspective. The CBECI offers some interesting comparisons such as, for example, the closest real-world analogue of Bitcoin is gold, and it is interesting to note that gold mining consumes 131 terawatt-hours slightly more than its

digital counterpart i.e. Bitcoin. Global air conditioning around the world consumes 2199 terawatt-hours which is 16 times more than Bitcoin, global data networks consume 250 terawatt-hours, global data centers consume 200 terawatt-hours, televisions and lighting in the US consume 60 terawatt-hours each.

However, power usage and environmental impact are not necessarily related, indeed it is vital to discern between them. The former pertains to the analysis undertaken in Section 5, but what really counts for environmental well-being is the latter. Thus, the energy mix employed by miners. According to the CBECI, 76% of miners claim to use renewable energy as part of their energy mix, and 39%of mining activities' total energy consumption comes from renewable sources.

6.2 Blockchain as a socioeconomic system

Assuming that miners are profit-maximizing economic agents, honesty is the most rational strategy, and consequently Bitcoin could be considered not so much a technical innovation as a carefully calibrated socio-economic system relying on a complex combination of economic incentives.

But how much energy should a blockchain consume? The answer to this question also relies on the factors taken into account; the energy discussion around the mining of cryptocurrencies remains fierce, but their social value is frequently overlooked. From a Western

perspective, as a developed and consequently privileged nation, it is natural that energy consumption be the primary focus. However, it is also crucial to evaluate a variety of societal factors that affect 70percent of the world's population. Only 30% of the world's population has access to "the basic principles of a liberal democracy: freedom of expression and belief, private property and a relatively stable economic system" (The Digital Economy, March 2022). There are 1.2 billion people in the world living in hyperinflation, and many are using cryptocurrency to make up for it. With the advent of cryptocurrencies, for the first time, people outside the 30% have a choice. They have the chance to attain autonomy and financial freedom. Neglecting these socioeconomic dimensions of cryptocurrencies could derail a purely energy examination of the technology.

That it does is inherent to how Satoshi Nakamoto's project was developed, which through the PoW consensus process enables the continuation of DLT without relying on a centralized organization, so assuring network security and a fair and transparent distribution, as it should be for any utility. The latter are tolerated because they contribute to society and are essential. This is precisely how it may be with Bitcoin, especially for countries with unique circumstances or where independence, autonomy, and transparency are impossible. Below is a comparison of the energy usage of several utilities and Bitcoin. The energy debate, however, has been limited to the use of Bitcoins and no other utilities; this perspective must be revised. The energy consumed by Bitcoins serves an extremely specialized purpose.

6.3 Energy Transition: The Cryptocurrency sector can lead the change

Contrary to popular belief, a key aspect of the energy transition and the expansion of investments in renewables is precisely the development of cryptocurrencies.

As we can read from the Bitcoin Clean Energy Initiative (BCEI), there are two primary factors to consider: the excess or waste of energy inherent to renewable sources and the adaptability of the Bitcoin network, which might serve as the sole purchaser of this energy. Together, they could result in an increase in solar and wind power generation capacity, so facilitating the energy transition and improving the efficiency of systems. BCEI contends that "today's energy asset owners can become tomorrow's critical Bitcoin miners." Not only is there a vision for society, but Bitcoin is mentioned as a means for the energy transition. "Bitcoin mining provides a chance to speed the worldwide transition to renewable energy by functioning as a complimentary technology for the generation and storage of clean energy". Reference is made to the production of renewable energy from wind and photovoltaics, which are the least expensive sources of energy today the actual strength resides in the fact that one technologywould aid the other and that, when combined, they mightlead to a significant improvement in the energy transition. Bitcoin mining plays a crucial rolebecause, as a flexible load, it has the potential to completely or substantially resolve the problems of grid intermittency and congestion produced by solar orwind power generation. Moreover, the increased dissemination of the latter would result in an increase

in efficiency due to the massive investments made in these technologies, but it would also reduce marginal production costs to nearly zero. Intermittency is a major drawback of solar and wind energy compared to more expensive baseload sources such as natural gas and nuclear power. This results in what the energy industry refers to as the "duck curve. "Intermittency is one of the fundamental issues with renewable energy sources. When citizens return home in the early evening, we have the highest demand, but the lowest production. Thus, there is a mismatch between supply and demand, which, when combined with the congestion of the power networks (which can be compared to highway traffic), results in the waste of a great deal of energy. The seasons also contribute to this disparity; in summer, the sunshine's brighter than in winter. In addition, wind and PV parks are frequently located in rural locations, where nature can be exploited to its fullest extent, but this poses a difficulty due to low demand (from rural end users) and grid transmission capacity. Due to these difficulties, there are even high-powered (up to 200 GW) wind or photovoltaic parks that are separated from the grid and therefore inoperable.

Bitcoin miners, on the other hand, are a great complement to renewable energy and storage technologies. As previously stated, there will always (or at least soon) be an issue of energy storage and dissipation. We believe that by integrating miners with storage systems (which can nearly entirely handle the daily intermittency of renewables) and renewable energy generation, it could:

1. Increase the quantity of renewable projects and increase the profitability of all green investments made in the sector.

2. Permit the construction of solar and wind installations prior to the completion of extensive grid connectivity studies, as Bitcoin miners can absorb the energy until it can be sold to the system.

3. Not dispersing excess energy but having a system that harnesses this additional energy to deal with days when demand can't be met is a method of avoiding energy waste.

Obviously, it should be highlighted that in this instance, under the overall system described above, the miners would have access to this additional energy.

Clearly, in such a scenario, a vicious circle would be created, with increased investment in renewable energy leading to an acceleration of the energy transition. In addition, Bitcoin mining would have no impact on total consumption, or at worst a negligible impact. Finally, the amount of investment stated previously would result in a fall in the levelized cost of energy (for wind and photovoltaics), which would make their adoption easier and more profitable over time. This would further broaden their use, which would become highly cost-effective, and one may explore employing hem for further valuable greenhouse gas removal applications (CO2removal from the atmosphere, water desalination, green hydrogen production, etc.)

Obviously, there would also be a change towards a significantly more environmentally friendly approach for Bitcoin mining. Clearly, the transition to green will not be complete and instantaneous; miners will continue to be connected to the grid and mine cryptocurrencies while gradually shifting to a decentralized and green production that could strengthen the security of Bitcoin's blockchain.

Thus, following the BCEI, the key players in the future of the energy transition are, of course, the owners of energy assets, but also and especially because they are converging with the cryptocurrency markets (Bitcoin in particular), which can boost clean energy production through large-scale investments, efficiency improvements, and simultaneous synergy with cryptocurrency mining.

7. Conclusions

In an era of energy transition where the environmental problem is becoming increasingly present, the development of innovation and the emergence of cryptocurrencies have raised many concerns regarding energy consumption and environmental footprint. This study has multiple objectives, starting with ananalysis of the energy consumption of blockchain regardless of its domain of application. Specifically,the analysis begins by identifying the major consumptionfactors and then calculating their consumption specifically. The results of this analysis are unequivocal: among the three sources of energy consumption of a blockchain, only one could be of concern from an environmental point of view, the PoW consensus mechanism. The analysis specifically led tothree sources of blockchain consumption and several results:

1. The communication messages between the various nodes of the blockchain that require less than 1 kW of power (equivalent to the output of a small photovoltaic panel installed on the roof of a domestic building) and about 5MWh in a year.

2. The energy consumed for storing the distributed ledger, with its many replicas. The calculation resulted in a consumption range of at most a few GWh per year or 400 kW average power (about the same as a modern wind turbine).

3. The PoW consensus mechanism has an annual energy consumption of more than 200 TWh per year, equivalent to an average power of about 10 GW (like the power produced by 10 nuclear power plants).

From the data obtained, it is immediate that the PoW consensus mechanism has a significantly higher energy consumption, which leads the other two consumption factors to be neglected. This consumption moves with the reward for miners and thus with the price of the underlying cryptocurrency. Without a limit on the price of this cryptocurrency, it is not possible to determine a theoretical upper limit for the energy consumption of the PoW consensus mechanism.

One action that can be taken to reduce consumption is to modify the consensus mechanism as some cryptocurrencies (Tezos, EOS, TRON) have already done and to use the PoS consensus mechanism. Even the second largest cryptocurrency by capitalization, Ethereum is making this transition. Of course, governments play a decisive and fundamental role in this; for example, they could impose regulations to impose substantial taxes on those who use the PoW method, discouraging this use.

Another solution that was addressed in Section 6 is the possibility of harnessing dissipated or unused energy from renewable sources such as wind and photovoltaics. This utilization would have many advantages: from solving grid congestion problems, to decreasing the marginal cost of renewable energy production systems, which would allow for a boost in their production and

utilization, and a cascade of considerable investment, research and increased efficiencies. On the other hand, the use of cryptocurrency miners as a flexible load for the electricity grid could exploit the excesses of the grid and continue to expand considerably, without major environmental problems, indeed fueling the energy transition.

The research also dwells on the whole innovative aspect of blockchain technology and how cryptocurrencies represent on the one hand an 'affront' to current financial systems, and on the other hand an innovation that could help sociality especially when it comes to the less affluent. We know how the power of today's banks and financial institutions govern the entire global economy, but not only that, for these reasons the advent of decentralized finance as we have seen is not and will not be easy. As was done in the study, it is important to try to consider a multitude of aspects when talking about this innovation, because as such it has an impact on everything around us. Especially next to the energy and environmental aspect, one should not forget the social one, which could be affected in a very positive way with the advent of cryptocurrencies.

To conclude, blockchain is an innovation of enormous scope and as such should be approached with caution. As far as the energy discourse is concerned, besides the problem of PoW consumption, what will happen once we all use it in different areas of our lives? What will happen when the networks are adopted by millions of people and transactions? What else should we worry about? Which of the various applications of blockchain could take hold in the near future?

References

- *Bitcoin.org. "Running A Full Node – Bitcoin." 2022. https://bitcoin.org/en/full-node.*
- *Bitcoin Clean Energy Initiative. 2021. *BCEI White Paper.pdf(ctfassets.net)*
- *Bitnodes. "Global Bitcoin Nodes Distribution." https://bitnodes.io/.*
- *Blockchain.com. "Average Block Size (MB)."*
- *Blockchain.Com. https://www.blockchain.com/charts/avg-block-size.*
- *Blockchain.Com https://www.blockchain.com/charts/blocks-size.*
- *Bouri, Elie, Rangan Gupta, Aviral Kumar Tiwari, and David Roubaud. "Does Bitcoin Hedge Global Uncertainty? Evidence from Wavelet-BasedQuantile-in-Quantile Regressions." 2017. https://doi.org/10.1016/j.frl.2017.02.009.*
- *Braun-Dubler, Nils, Hans-Peter Gier, Tetiana Bulatnikova, Manuel Langhart, Manuela Merki, Florian Roth, Antoine Burret, and Simon Perdrisat. "Blockchain: Capabilities, Economic Viability, and theSocio-Technical Environment." 2020. https://www.ta- swiss.ch/en/blockchain.*
- *Brière, Marie, Kim Oosterlinck, and Ariane Szafarz. "Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoin."2015. https://doi.org/10.1057/jam.2015.5.*
- *Buterin, Vitalik. "Ethereum Whitepaper: A Next-Generation SmartContract and Decentralized Application Platform." 2013. https://whitepaper.io/document/5/ethereum-whitepaper.*
- *CBECI. "Cambridge Bitcoin Electricity Consumption Index (CBECI)." 2021. https://cbeci.org/.*
- *Chaum, David. "Blind Signatures for Untraceable Payments." 1983.https://doi.org/10.1007/978-1-4757-0602-4_18.*
- *Chen, Yan, and Cristiano Bellavitis. "Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models."2020. https://doi.org/10.1016/j.jbvi.2019.e00151.*
- *Coroamă, Vlad C. "Investigating the Inconsistencies among Energy and Energy Intensity Estimates of the Internet – Metrics and Harmonising Values." 2021.https://www.aramis.admin.ch/Default?DocumentID=67656.*

- *Coroamă, Vlad. "Blockchain energy consumption". 2021.* Default(admin.ch)
- *De Cristofaro, Eugenio. "La Blockchain oltre le Cryptovalute. Analisi di altri ambiti di applicazione: i casi Adamantic e Mnemonica". 2019. La blockchain oltre le Cryptovalute. Analisi dialtri ambiti di applicazione i casi Adamantic e Mnemonica - De Cristofaro.pdf*
- *Digiconomist. "Bitcoin Energy Consumption Index." 2021.https://digiconomist.net/bitcoin-energy-consumption/.*
- *Douceur, John R. "The Sybil Attack." 2002.https://doi.org/10.1007/3-540-45748-8 24.*
- *Ethereum, Developer Resources. "Ethereum Accounts." 2021. https://ethereum.org/en/developers/docs/accounts/.*
- *Guerra, Raquel. "MEPs Push for Cryptocurrencies Generated viaSustainable Technology." 2021. https://www.endseurope.com/article/1718188/meps-push-cryptocurrencies-generated-via-sustainable-technology.*
- *Hertig, Alyssa. "What Is DeFi?" CoinDesk (blog). 2020. https://www.coindesk.com/what-is-defi.*
- *Hintemann, Ralph, and Simon Hinterholzer. "Energy Consumption of Data Centers Worldwide - How Will the Internet Become Green?" 2019.http://ceur-ws.org/Vol-2382/ICT4S2019_paper_16.pdf.*
- *Kamiya, George. "Bitcoin Energy Use - Mined the Gap." 2019. https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap.*
- *Krause, Max J., and Thabet Tolaymat. "Quantification of Energy andCarbon Costs for Mining Cryptocurrencies." 2018. https://doi.org/10.1038/s41893-018- 0152-7.*
- *Lamport, Leslie. "The Weak Byzantine Generals Problem." 1983.https://doi.org/10.1145/2402.322398.*
- *Leone, Lucrezia. "Central Bank Digital Currencies: impact on monetary and financial system". 2019. *Central Bank Digital Currencies_ impact on monetary and financial system - Leone .pdf*
- *Luu, Loi, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. "A Secure Sharding Protocol For OpenBlockchains." 2016.*

https://doi.org/10.1145/2976749.2978389.

- Martin, Katie, and Billy Nauman. "Bitcoin's Growing Energy Problem:'It's a Dirty Currency.'" 2021. https://www.ft.com/content/1aecb2db8f61-427c-a413- 3b929291c8ac.
- Masanet, Eric, Arman Shehabi, Nuoa Lei, Sarah Smith, and JonathanKoomey. "Recalibrating Global Data Center Energy-Use Estimates." 2020. https://doi.org/10.1126/science.aba3758.
- McKenz, André François. "Sustainability Solution or Climate Calamity? The Dangers and Promise of Cryptocurrency Technology."2021. https://news.un.org/en/story/2021/06/1094362.
- Merkle, Ralph C. "A Digital Signature Based on a Conventional Encryption Function." 1988. https://doi.org/10.1007/3-540-48184-2 32.
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008. https://bitcoin.org/bitcoin.pdf.
- Raschi, Alessandro and Senni, Luca. "Blockchain conceptualisationand theoretical implications: a case-base approach". 2018. Blockchain conceptualisation and theoretical implications a case based approach.pdf
- Sorrentino, Sara. "Criptovalute: funzionamento, tecnologie epossibilità d'investimento". *Criptovalute funzionamento, tecnologie e possibilità d'investimento - Sorrentino.pdf
- Stoll, Christian, Lena Klaaßen, and Ulrich Gallersdörfer. "TheCarbon Footprint of Bitcoin." 2019. https://doi.org/10.1016/j.joule.2019.05.012.
- Trionfo, Francesco. "Bitcoin, Blockchain e Cryptocurrncies". 2018. *Bitcoin, Blockchain and Cryptocurrencies - Trionfo.pdf
- Vries, Alex de. "Bitcoin's Growing Energy Problem." 2018.https://doi.org/10.1016/j.joule.2018.04.016.
- Wüst, Karl, and Arthur Gervais. "Do You Need a Blockchain?" 2018.https://doi.org/10.1109/CVCBT.2018.00011.
- Why the debate about crypto's energy consumption is flawed | WorldEconomic Forum (weforum.org)