Department of Economics and Finance

Chair of Financial Markets and Institutions

Blockchain Technology: Applications Beyond Cryptocurrency

SUPERVISOR

PROF. STEFANO DI COLLI

CANDIDATE

SARA CECIARELLI

ID: 225641

ACADEMIC YEAR 2019/2020

Table of Contents

INTRODUCTION

Formally born in 2009 with the creation of Bitcoin thanks to Satoshi Nakamoto, cryptocurrencies have quickly captured the attention of the world public. In recent years, we have often heard the media mentioning the term bitcoin. Sometimes for the incredible fluctuations in value, sometimes for its use in criminal activities.

Today, there are more than 2000 cryptocurrencies circulating in the market, and they all have in common the technology on which they are based, that is the blockchain.

However, blockchain applications are not limited to cryptocurrencies. In fact, blockchain is already considered one of the most innovative technologies available to businesses.

This study aims to provide a detailed description of the principles behind this technology, in order to understand and give practical examples of how it is possible to take advantage of it in several applications.

One of the main goals of the blockchain technology is allowing somebody, in every part of the world, to carry out transactions without the need to rely on any central institution. It is distributed on a network consisting of interconnected devices, called nodes, communicating with each other and sharing informations.

One of the main reasons that led to the birth of the blockchain technology, was the search for a system without errors and inherently devoid of problems that have always plagued centralized institutions, such as corruption, and lack of fairness when making choices.

Traceability, immutability and security are the three characteristics of the blockchain that make it a perfect "backstage" for many changing technologies that may heavily impact the way we consume, govern, communicate, educate and manage.

These blockchain's benefits have sparked a huge interest in different areas. To this concern, the second section of this study will focus on the main aspects of the new socio-economical paradigm, such as Smart Contracts, DAO and Token Offerings. Some of the most important cross-industry applications will be analyzed, providing practical examples on how the blockchain has proven to be the best mean to significantly increase efficiency in the financial, supply chain, government, education and energy sectors.

It will be a clear overview on how this technology is rapidly becoming a strategic priority for many companies, with the promise of reducing costs and inefficiencies, radically transforming the business models we know today.

One of the aspects that differentiates the "physical" from the digital world, is the extreme ease with which it is possible to copy data and information.

This feature is in stark contrast to the properties that the money must have. For this reason, up to now all the forms of digital money have always had to rely on a central authority, such as a bank that acted as the sole holder of the truth, preventing digital money from being duplicated and spent multiple times (the double spending problem). For the first time, thanks to blockchain, the double spending problem can be solved without relying on a central authority.

However, the revolutionary aspect of this technology is not limited to this. The blockchain allows us to face one of the cardinal aspects of our society in a completely different way: the problem of trust. The last chapter of this study will hence describe carefully the Bitcoin protocol, so to understand how transfers of value take place. Moreover, the consensus models that can be adopted in a blockchain will be explained in detail together with a list of the most famous cryptocurrencies as of today.

1 CHAPTER 1: BLOCKCHAIN TECHNOLOGY

1.1 DEFINITION AND OVERVIEW

In the last few years, the number of investors and enthusiasts of cryptocurrencies has increased significantly. It seems, however, that people tend to dwell on the transaction's innovation in the financial sector. What is important to highlight is that cryptocurrencies represent only the tip of the iceberg if compared to all the variety of innovative applications offered by the blockchain technology.

There exist many definitions regarding this technology. Some of them focus on the structure, others on the technology behind it, or its applications in the business world and society. All of these aspects are equally important in order to give a comprehensive overview of the subject.

In the technical language this technology is described as a decentralized and distributed communication protocol that leverages cryptography. Unlikely, for those who are not familiar with the concept, it is not very explanatory.

In order to better express the idea, we can define the blockchain as a particular type of database, specifically a *distributed ledger technology (or DLT),* which has certain unique properties. It is structured as a series of *blocks* responsible for the storage of records of data, usually referred to as *transactions*. It is possible to add other blocks of information, but they can't be either modified or removed. By looking at the most recent block, it is possible to check that it has been created after the last. So, continuing down the “chain”, we'll reach the very first block, known as the genesis block.

The concept of blockchain is common to almost all the blockchain systems[1], but the design of these blocks can differ depending on the purpose for which the blockchain was designed. Blocks can have different dimensions depending on the number of transactions they contain and can memorize different pieces of information.

At this point of the definition, some questions may arise. For example:

- How are these blocks connected?
- Who is entitled to add new blocks?
- How blocks and data herein are made available to the network?

To answer the above questions, in the following section we will go in a more-in-depth view of the key aspects of the technology.

[1] Later in this chapter, a distinction between the different types of blockchain will be provided

1.2 HASHING

Simply put, we can think about the hash function like a digital fingerprint of a digital content.

The data is passed through a mathematical function to produce an output (a hash) that's always the same length. In other words, the input of a hash function can be anything (an mp3 file, a pdf, an entire blockchain), but the output will always have a finite number of bits. The fundamental concepts that we have to keep in mind are:

- The same input always produces the same output, which is a hash, that has the form of a string of numbers and letters.
- Even the slightest modification in the input produces a drastic change in the output of the function.
- Is a one-way function.

1.1 Table - examples of a hash function output[2]

INPUT	HASH FUNCTION	OUTPUT
Sara Ceciarelli	SHA-256	82e394a407f70bdad49ed1a90f4df1fe1a1c4ee6e6da11416892b62d20b98987
sara ceciarelli	SHA-256	935e79ebed64262c4395abd68c95dee48614c0f3f15d92f8a3294a9c7a45b5c5

SHA-256 is one of the most famous hash functions.

In blockchain it can be defined as the glue that holds blocks together. Each block in the chain consists of two main parts: the header and the body. Transactions are enclosed in the body of the block and the header. In the header, each block refers to the previous block in the chain by its hash and contains a timestamp to ensure chronological order in the chain.

The block hashing is the mean by which to ensure the integrity of the block and eventually of the chain itself.

[2] https://xorbin.com/tools/sha256-hash-calculator

1.3 NETWORK

One of the main goals of the blockchain technology is allowing somebody, in every part of the world, to carry out transactions without the need to rely on any central institution (in the case of a monetary transaction, a bank).

In order to do so, a blockchain has to be distributed on a network. We can define a network as a group of interconnected *nodes*, i.e. machines that communicate with each other exchanging informations.

1.3.1 Nodes in a Peer-to-Peer Network

The blockchain technology is characterized by a Peer-to-Peer network consisting of a group of devices collectively storing and sharing files. The devices that make up the network are called nodes and they are points where messages can be created, received, or transmitted. Blockchain nodes act as communication points that may perform different functions. Any device that connects to the network may be considered as a node in the sense that they communicate somehow with each other.

In this kind of network each node holds a copy of the files, so there is no need for a central administrator Because of these reasons, P2P networks tend to be more efficient and very resistant to cyberattacks, due to the fact that there's no single point of failure.

Hereby we will discuss two different types of nodes: full nodes and light nodes.

- **Full nodes** are the ones that really support and provide security, which makes them indispensable to the network. Usually, a full node downloads a copy of the blockchain with every block and transaction and makes sure that the blocks are following the rules set by the system. If an anomaly were to occur, the block (or the transaction) would be simply denied, even if considered valid from the other nodes in the network.
  A full node is, to all intents and purposes, independent. It doesn't require any other node's trust and rigorously follows the rules.
  The use of a full node is the safest way to interact with a blockchain, but it can be quite inconvenient, since it requires the download of an entire blockchain (in the case of Bitcoin's blockchain we are talking about 270 gigabytes as for April 2020)[3].

- **Light nodes** do not memorize the whole blockchain but receive only the data they need from a trusted node (a full node). Consequently, the use of this type of node implies the delegation of trust

[3] https://www.blockchain.com/charts/blocks-size

from a third party (the full node), in exchange for the ease of use. A light node can be, for example, a wallet on a mobile device.

Beside data decentralization, one of the main reasons that led to the birth of the blockchain technology was the search for a system without errors and conditioning that can be attributed to the human race.

A full node flatly follows the rules imposed by the system, regardless the decisions of the other nodes. It follows a system inherently devoid of problems that have always plagued centralized institutions, such as corruption, and lack of fairness when making choices.

1.3.2 Architecture

In a blockchain system, the network is a fundamental component. Looking at the network structure and the role of each node, it is possible to identify three network models: centralized, decentralized and distributed.

1.2 Figure - Source: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

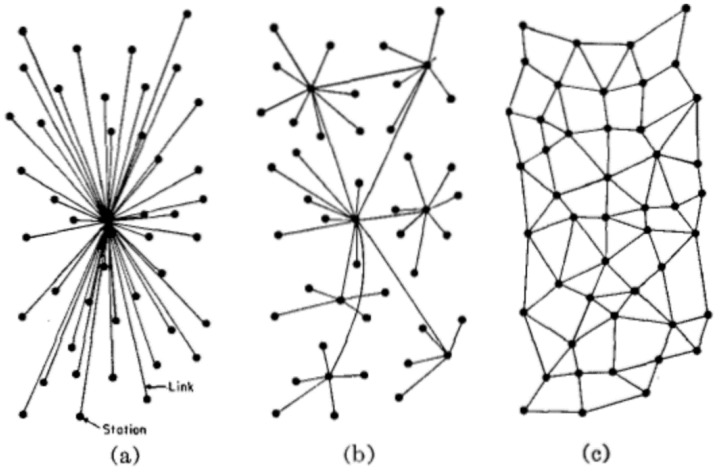


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

The degree of centralization is a concept which gives us the possibility to analyze a multi-level system. We will categorize the systems based on their centralization from the point of view of the architecture, the authority (political) and the logic[4].

From the point of view of the **architecture,** a centralized network is an infrastructure that has a single point of failure which, if compromised, would prevent the entire system to function correctly (for example, the client-server model).

[4] The founder of Ethereum, Vitalik Buterin, also uses this subdivision. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

In a decentralized network, the resources are distributed and possibly copied by the nodes of the network and, as a consequence, every application is runned by all the participants which makes it impossible to have a single point of failure. In other words, in order for a decentralized system to stop functioning, is necessary to "shut-down" each node (for example, in the Bitcoin blockchain, you will have to shut-down all 10.000 nodes)[5].

A network subjected to a centralized **authority** is characterized by a central entity which controls the data, the operations and the users. To give an example, Amazon, Google, Facebook or any bank are all systems characterized by a central authority. This authority is the one that makes the rules in the system and has the power to impose them to the participants, demanding unconditional trust.

In a network subjected to a decentralized authority there is no central domain and all the nodes are considered equal.

To distinguish between a **logical** centralization/decentralization a simple heuristic would be: if you were to cut the system in half, including providers and users, will both halves continue to operate as independent units?

An example of a logically decentralized network could be emails: if I delete an email from my account, it doesn't mean that I'm also erasing it from the accounts to whom I've sent it.

Now that we have explained all the three aspects, we can contextualize them. Referring to Vitalik Buterin's article on medium.com we can say that Blockchains are “politically decentralized”, given the absence of a central authority. “Architecturally decentralized”, as there is no infrastructural point of failure, and “logically centralized” since there is only one “commonly agreed state” and the system behaves like a single computer.

In order to conclude this argument, the last thing to mention is that the Blockchain network is also **distributed.** In a distributed network, data and computations are, in fact, distributed to one or more nodes, but the authority remains centralized. In order to minimize risks and management difficulties, distributed networks do not have a one big server or database, instead they have many data centers all over the world.

[5] Beedham, M. (2019, March 12). All you need to know about Bitcoin network nodes. Retrieved June 18, 2020, from https://thenextweb.com/hardfork/2019/03/01/bitcoin-blockchain-nodes-network/

1.4 TYPES OF BLOCKCHAIN

So far, we understood how the blockchain technology can be applied to any scenario where a distributed control structure is required. However, in some cases a blockchain's authority cannot be decentralized, but tends toward centralization. To be specific, according to how the authority is managed, there exist three different types of blockchain.

Public Blockchain (permissionless)

This model is doubtless the most famous and used. Decentralization is a key aspect since every attempt of centralization would be defined as a weakness of the system, showing a potential point of failure. It doesn't exist a single authority, everyone can join the open network and there is no discrimination based on origin, destination or content. This model is neutral, and everyone has the possibility to explore and verify each transaction. This architecture allows each node of the network to actively contribute to updating the data registered in the database and obtain a copy of each operation performed on it. When we talk about blockchain, usually we refer to public blockchains and the most famous are Bitcoin and Ethereum.

Private Blockchain (permissioned)

A private blockchain is a permissioned blockchain: exactly how blockchains shouldn't be, that is, centralized. Private blockchains have access controls to restrict the number of people that can participate in the network. Since one or more entities control the network, this kind of blockchain relies on third parties to transact. Private blockchains, in turn, can be subdivided into:

- Private permissioned
- Public permissioned

In the private one, you need to be authorized in order to read the register and access the transactions. In the public permissioned, all the nodes that make up the DLT (Distributed Ledger Technology) are able to read data and submit transactions.

In general, the possibility to read the register can be guaranteed to everyone or can present some limitations. They are therefore controlled and restricted to one or more central authorities. Typically, private blockchains are used by big enterprises and institutions for greater reliability: in this case they are defined as "consortium blockchains". A consortium blockchain would be most beneficial to organizations that operate in the same industry and require a common ground on which to carry out transactions. Joining a consortium in this case could be beneficial as it would allow those organizations to share insights with other players. Some examples are:

- Hyperledger, founded by Linux, is mainly focused on providing technological support for the blockchain revolution and is supported by many multinational companies (like IBM, Cisco, Intel, J.P. Morgan, etc.).
- R3 leverages their open source blockchain platform "Corda" to solve real business problems in highly regulated markets, working alongside some of the world's leading financial institutions (such as Banca d'America, Goldman Sachs, Citigroup, etc.).

Fundamentally, private, public and consortium, are not in contrast with each other - they are different technologies:

- Well-designed public blockchains tend to excel when it comes to censorship and resistance. These are the ones that work best for security assurances on transactions settlements - or *smart contracts*.
- Private chain can be ideally deployed in situations where an organization must remain in control and information kept private.
- Consortium chains mitigate some of the risks that arises with private chains by removing decentralized control. A smaller number of nodes generally allows those chains to have high performances. Consortium are likely to appeal to organizations that want fast communications amongst one another.

There exists a myriad of blockchain options made available for businesses and individuals engaging in various activities. Depending on the use case, users will need to select that which is best suited to achieving their own goals.

1.5 SUMMARY OF CHARACTERISTICS

After explaining the basic structure and concept beyond the technology, we can now summarize some of the most important characteristics of the blockchain technology:

Traceability

We have seen how the database is divided in blocks and that each block is linked with the others. In this way each operation initiated inside the network has to be validated by the nodes that make up the structure. The nodes can perform multiple tasks, for example: monitor the operations/transactions of the other nodes, check the consistency of the operations and eventually approve them.

Immutability

The database that includes all the operations can be downloaded and consulted by every node that joins the network. Immutability is the ability for a blockchain ledger of remaining a permanent and unalterable history

of transactions. This feature is important because provides integrity and can bring an unprecedented level of trust among businesses.

Security

The security of the system is guaranteed by cryptography applied to transactions. Cryptography is a process that encodes a message or file so that it can be only be read by certain people. This mechanism determines the exclusivity of the message being sent or received. Security is also guaranteed by the fact that all the informations concerning the transactions are shared and accessible by all the participants of the network.

The combination of all the characteristics explained above is what makes the blockchain such a perfect "backstage" for many changing technologies and will impact the way we consume, govern, communicate, educate and manage. Blockchains can enable faster and more reliable automated communication. It could substantially reduce bureaucracy and increase security, efficiency and transparency. With cybersecurity, being all data verified and encrypted in blockchain, we could easily prevent and stop unauthorized changes and hacks. With the advent of blockchain, many organizations could create a centralized and secure database, store records and share them strictly with authorized entities.

Hereon, I will discuss the most popular cross-field applications of this technology, beyond the one of cryptocurrency. Lastly, the first and most well-known blockchain application will be explained in detail – that is, Bitcoin. In turn, a detailed description of some of the most popular cryptocurrencies will be provided, with the aim of delivering a deeper insight of how the blockchain technology has been adapted to meet different needs.

2 CHAPTER 2: BLOCKCHAIN APPLICATIONS

Historically, when society was to face a new revolutionary technology, the first reaction has always been that of mistrust. It happened with cars, with electricity and with Internet. The issues that new technologies have to face are many, for example a non-complete development, an unsuitable infrastructure ecosystem or an adverse legislation.

Blockchain is perfectly part of this paradigm. It exists a technology able to remove intermediaries and exchange value without the need of a central authority. But it misses the right infrastructure that will allow the technology to proliferate.

2.1 THE SOCIO-ECONOMICAL REVOLUTION

Not long after the diffusion of the blockchain technology it was clear how Bitcoin was not the only revolutionary application at stake. Hence, with the term "smart economy" it is identified blockchain and smart contracts' applications to the economic processes.

The main components of this smart economy are:

2.1.1 Smart Contracts

The term "smart contract" was first used by Nick Szabo in 1997. Szabo's intention was to use a distributed ledger to store contracts.

To make a practical example we can take into account a fundraising platform, where and hypothetical product team can create e project and set a funding goal to start collecting money from potential investors. This platform essentially works as a third party that sits in between the product team and the supporters, which implies that both the parties will have to trust the platform with their money. With smart contracts, it is possible to build a similar system which doesn't require a third party to manage the process.

Being smart contracts stored in the blockchain, they inherit some interesting properties:

- Immutability, which means that once a contract is created it can never be modified, meaning that the code of the contract cannot be tempered.
- They are also distributed, meaning that the output of the contract is validated by every participant on the network.

Smart contracts can be applied to many different sectors. Banks, for example, use it to issue loans or to offer automatic payments, postal companies could use it for payment on delivery, insurance companies to process certain claims, and so on.

As for now, there are many types of blockchains supporting smart contracts and the biggest one is Ethereum.

Moreover, the blockchain technology may change the way we transact assets and think of ownership. **Smart property** allows for the digitalization of assets whose ownership is controlled by the blockchain, through

smart contracts. **Digital identity**, on the other hand, allows for the digitalization of a person or organization's identity which is then managed on the blockchain. **Token model** is an economic model based on the use of cryptocurrencies for monetary transactions.

Smart economy can be seen as an attempt of applying the principles of the blockchain technology to an economic system. A practical example of this are DAO.

2.1.2 Decentralized Autonomous Organizations (DAO)

DAO's tackle a well-known governance problem: the principal-agent dilemmas of organizations and moral hazards caused by asymmetric information.

In traditional companies, the relationship between the agents of a company and the organization is regulated through a legal contract, which sets forward their rights and obligations. This legal contract is enforced by a legal system, subject to the laws of the country they reside in. Legal contracts main functionality is to define who can be sued and for what in the events when someone did not stick to his/her end of the bargain.

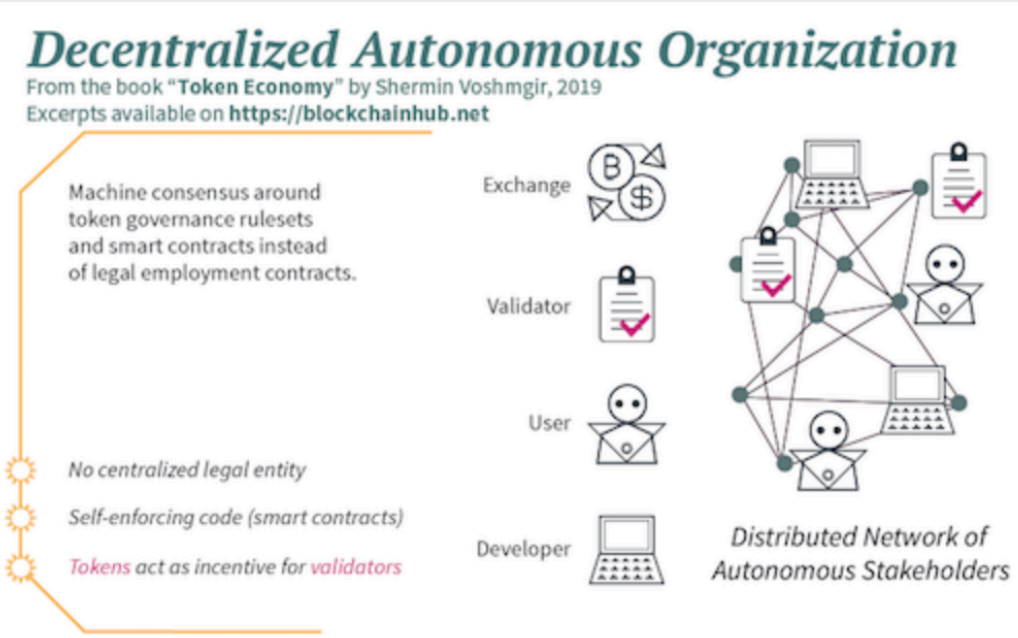
In DAOs, on the other hand, all agents interact with each other according to a self-enforcing protocol and individual contribution is incentivized with a token. Members of a DAO did not enter a legal contract, but they are driven by incentives and fully transparent rules that are written into the software, enforced by machine consensus. In other words, a DAO is a computer code to which a set of smart contracts are connected and function as a governance mechanism.

DAOs provide an operating system for people and institutions that may live in different countries, and therefore be subject to different jurisdictions. In a DAO all transactions of the organization are recorded and maintained on a blockchain making it transparent and, theoretically, incorruptible.

Within a DAO, the interests of members and the organization are aligned, and proposals are the primary way for making decisions, which are voted for by majority consensus.[6]

[6] What is DAO - Decentralized Autonomous Organizations. (2019, August 30). Retrieved June 16, 2020, from https://blockchainhub.net/dao-decentralized-autonomous-organization/

Figure 3.1 – Source: https://blockchainhub.net/dao-decentralized-autonomous-organization/



The most infamous DAO project was "The DAO", created by Slock.it in 2016[7].

The idea of the DAO was to raise funds from investors for projects by submitting a proposal for funding using the DAO funds. The proposal has to go through a verification process and once it passes the check, if approved by a quorum of 20% of all tokens, the DAO automatically transfers the tokens to the smart contract that represents the proposal.[8]

DAO's initial offering took place in May 2016 and became the biggest crowdfunding project up to that time, raising 12.7 million Ether (more than 150 million USD back then). However, on 16 June 2016, the DAO got hacked.

The idea was to safeguard the minority of the investors by enabling them to retrieve their funds whenever a proposal got approved despite their objection. The solution was implemented by the creators as an ability of the DAO to split in two, creating a child DAO where the minority of the investors could store their tokens.

Once the split procedure has been initiated through a proposal, a split proposal must have at least 1 week of debate time, 27 days before the Ether can be moved to a child DAO and even after that, moving funds into the child DAO to a private account took 14 days. Simply put, once a token holder decides to split a DAO, he/she needs to wait at least 48 days before transferring the funds in a private account.

[7] All codes regarding the DAO, including samples of smart contracts and proposal offers, can be found at https://github.com/slockit/DAO.

[8] Tual, S. (2016, April 12). A Primer to Decentralized Autonomous Organizations (DAOs). Retrieved June 11, 2020, from https://blog.slock.it/a-primer-to-the-decentralized-autonomous-organization-dao-69fb125bd3cd

However, once a split function is called, the code was written in a way to retrieve the Ether first and update the balance later. Additionally, there was no way to check if there was a recursive call[9]. Hence, the attacker who found this loophole, managed to repeatedly call the split function and retrieved the funds multiple times before the code would check the balance. Due to this practice, on 16 June 2016, the attacker managed to retrieve approximately 3.6 million Ether from the DAO fund. Ultimately, this event led to a controversial hard fork of the Ethereum blockchain.

2.1.3 The Evolution of the Token Offerings: ICO, IEO, STO

In the previous paragraph I've talked about how a person or an organization, can raise funds from supporters or investors on the blockchain. In the world of cryptocurrencies, a fundraising method of this type is properly named an ICO (Initial Coin Offering). An ICO is often compared to an IPO (Initial Public Offering). However, this comparison is somehow misleading.

An ICO is usually used for projects that haven't yet developed their own blockchain platform, their product or service. The payment is usually made with Bitcoin or Ethereum and in some cases fiat money are accepted. Investors participate in an ICO hoping that the project in question will be successful, increasing demand causing an increase in the value of the underlying tokens, hoping to receive a good ROI. In other words, ICO are more like crowdfunding to provide businesses with capital for their project and the investors that are investing tokens are not buying any shares of the company. On the other hand, IPOs are for established businesses offering shares of their private corporation to the public.

But why companies use ICOs? Because they can me a very efficient method to raise funds and venture capital raising. This method is very convenient for start-ups because it allows to raise funds based on an idea. A lot of these not consolidated small enterprises wouldn't be able to raise capital in any other way, given the unlikelihood by which financial institutions would not lend money based on a whitepaper, especially in the crypto scenario[10].

ICO popularity peak was reached in 2017 when 875 ICOs took place with total funds raised of more than 6 billion dollars[11]. However, a situation where the creation of an ICO is pretty straightforward and the collection of money is also easy, is aggravated by the fact that there is no one to guarantee that the project will go on, which makes the possibility of fraud the major downside of this practice. This is why many investors are moving away from ICOs and considering other crowdfunding methods such as IEOs and STOs.

---

[9] Expression used to indicate a function that calls itself.

[10] Binance Academy. (2020, January 19). Che Cos'è una ICO (Initial Coin Offering)? Retrieved June 12, 2020, from https://academy.binance.com/it/economics/what-is-an-ico

[11] ICOdata - ICO 2017 Statistics. (n.d.). Retrieved June 12, 2020, from https://www.icodata.io/stats/2017

With IEO (Initial Exchange Offering) we shift from a situation where unknown start-ups where offering their tokens on the market, to a new phase where a selection is applied. Exchanges act as guarantors for the projects. For taking this responsibility, the exchanges charge a fee calculated based on the visibility of the Exchange on the market, or they invest themselves on the project to increase and strengthen their ecosystem[12]. IEO is one of the most preferred methods for the majority of investors. However, the downsides of an IEO are the high investments minimums and a restricted choice of IEO platforms.

Another step forward to the token offerings evolution is the STO (Security Token Offering). Unlike ICO, a security token is asset-backed and complies with the regulatory governance. STOs are linked to an underlying investment asset just like stocks, bonds and other funds. These tokens are negotiable financial instruments with an attached monetary value and as such, are not traded on regular exchanges. The exchanges that offer security token trading must comply with regulations[13].

2.2 APPLICATION AREAS

In this paragraph, cross-industry impacts of the blockchain technology will be analyzed. The discussion has the purpose of giving insights on how the blockchain can be used in various situations.

2.2.1 Financial Services

The financial sector is the most discussed field for the application of the blockchain technology. Through the course of this study it was clear how blockchain, and more in general DLT can definitely increase efficiency in different aspects of the financial sector like payments, assets custody and trading.

Technological innovations in the sector have given rise to the so-called **Fintech**, which stands for financial technology and is used to describe how technology seeks to improve the use of financial services. Specifically, it refers to the set of products and services that are emerging thanks to the application of the latest technologies to the world of finance. Online banking and savings and investments services through app are some of the most common fintech innovations.

Services based on blockchain technology, however, are still going through the research and development phases, but could soon revolutionize several processes that affect our interactions with banks and other entities. This technology is finding wide acceptance in almost all sectors that provide some form of exchange of value.

[12] Evoluzione delle token offerings: Dalle ICO alle IEO e STO. (n.d.). Retrieved June 12, 2020, from https://www.brightnode.io/it/blog/evoluzione-delle-token-offerings-dalle-ico-alle-ieo-e-sto/

[13] What Is A Security Token Offering (STO)? (n.d.). Retrieved June 12, 2020, from https://cryptonews.com/guides/what-is-a-security-token-offering-sto.htm

A recent report produced by Acta Fintech, a communication and consultancy company operating in the fintech and blockchain sector, shed light on the current state of adoption of this emerging technology in the banking sector, taking into consideration the national and international scene. Some of the main uses of this technology in the banking world concern the need for greater security of agreements through Smart Contracts, the management of Digital Identity, the achievement of greater data transparency, the tokenization of physical assets and the transfer of cross-border funds.

A practical example of the application of technology, reads the report, is given by remittances which represent the largest flows of money to developing countries. According to the World Bank Group, the remittance sector has seen significant growth in recent years, increasing by 8.8% in 2017, and by 9.6% in 2018. The World Bank estimates that the current cost of sending a remittance of $ 200 is about 7% (global average). Considering that in 2018 the remittances worldwide reached $ 689 billion, 7% means approximately $ 48 billion paid in operating costs. In addition to the high costs, most remittance solutions are based on third party financial institutions and services. The need for several intermediaries makes the current system extremely inefficient. Not only for the costs related to the services but also for the long times of the transactions, which can take days or even weeks. The central goal of blockchain companies that deal with remittances is to simplify the whole process, removing unnecessary intermediaries and provide fluid and almost instantaneous payment solutions[14].

Among the most interesting examples presented by Acta Fintech in the document, in Italy **Hype** is the well-known smart contract connected to **Banca Sella.** The Hype card is a product of the Banca Sella Group, the first company in Italy to offer an e-commerce payment system since 1997. Its new creation is the rechargeable Hype card, equipped with an IBAN to make and receive payments, which was declared the best prepaid card in 2016. A survey conducted by Hype on a representative sample of its user base showed that as many as 13.5% of customers want the opportunity to buy and exchange cryptocurrencies. For this reason, in collaboration with the Italian startup **Conio**, Hype has developed a system that allows its customers to purchase Bitcoin. Trading will be conducted through the company's HYPE platform, and the bank acts as an intermediary to mitigate potential security risks. Users of the new service will also be able to purchase goods and services using cryptocurrency.

Continuing with the examples of application of the technology by banks and financial institutions of our country, in August 2018 **UniCredit** announced that it had successfully completed its first international transaction through the trade finance platform based on blockchain technology **We.trade**. “Through the use of a smart contract, the UniCredit has allowed the Asa Group, a manufacturer of metal packaging, to conclude the purchase of a tinplate consignment from one of its suppliers, Steelforce, which in turn is supported by Kbc Bank. in Belgium.”

[14] Report: Blockchain banking in Italia e nel mondo. (2020, May 28). Retrieved June 17, 2020, from https://actafintech.com/2020/04/01/report-blockchain-banking-italia-mondo/

Mediolanum is also one of the examples cited in the report. With the use of the Ethereum blockchain, Banca Mediolanum has successfully conducted the certification of the non-modifiability of the Non-Financial Statement. The adoption of this notarization process represents a further confirmation of the bank's commitment to make all stakeholders aware of the commitments, actions and performances in the economic, social and environmental fields.

2.2.2 Supply Chain

Supply chain is a network between suppliers and companies to produce and distribute products or services to the final buyer. The entities that operate in the supply chain include producers, vendors, transportation companies, retailers and more.

Supply chain includes, among other things, the procurement of raw materials and components necessary to obtain the final product. In the current global markets, these processes have become extremely complex, such that they often involve remarkable increases in the price of the product or a decrease in the quality.

In this complex scenario, the derived downsides could be many; such as the loss or manipulation of informations, the complex management of the logistic process, or the delays due to bureaucracy.

The aforementioned problems are clearly linked to a lack in transparency and traceability. Through the immutability and data securitization, it would be possible to store each step of the production inside the blockchain making the process clear and visible to all the authorized parties. In this way blockchain acts as a "single point of truth" for all the subsidiaries, partners and customers. Moreover, blockchain would be highly beneficial when it comes to the distribution and traceability of fresh products.

A practical example of the blockchain applied to the supply chain is Walmart, where the technology is applied in order to act faster in the case of an outbreak of food-borne disease and protect the livelihood of farmers by discarding produce coming from affected farms.

According to the Hyperledger case study, in October 2016, Walmart and its technology partner IBM announced two blockchain-based projects:

1. Tracing the origin of mangos sold in the US stores.
2. Trace pork sold in its China stores.

When these two projects turned out to be successful, Walmart wanted to expand its traceability project and started reaching out to other food companies. In August 2017, Walmart collaborated with IBM and other food industry players like Nestle and Unilever, to set up IBM Food Trust. By September 2018, Walmart was tracing over 25 products from 5 different suppliers using IBM Blockchain, built atop Hyperledger Fabric[15].

[15] How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric. Retrieved from https://www.hyperledger.org/learn/publications/walmart-case-study

Another interesting platform based on blockchain is **VeChain**, founded in 2015. VeChain is a blockchain application platform that focuses on the supply chain management, product traceability and anticounterfeiting. Initially built on Ethereum until it launched its own blockchain called VeChain Thor. VeChain combines the IoT technology with the blockchain to digitize the supply chain[16]. The basic idea is that of customers, or whoever wants to check the characteristics of the product, scanning a QR-code, RFID- or NFC-tag[17] and seeing through an app everything they need to know about the product. If you come across a spoiled product, the app will warn you and tell you why it's unsafe to eat. Through the unique ID tag attached to the product, the system is aware of their entire history. Sensors on the product collect data on its environment and that information gats attached to VeChain decentralized blockchain. Being the information added to the blockchain unchangeable, this creates an immutable record of the products' origins which can also help to stop counterfeiting[18].

2.2.3 Government Sector

Blockchain applications in the government sector and public administration are many. In recent time we have heard mainly about digital identity and how it would be possible to automate a series of processes regarding, for example, health, education, payment of taxes or in general to simplify a scenario with high levels of bureaucracy.

The proof of your identity is a basic requirement when it comes to opening a bank account, attending school, collect social security, seek legal protection and so on. These are all activities that allow a person to fully participate in their society and economy.

According to the World Bank, there are approximately 1 billion people lack a proof of legal identity in developing countries[19]. Here is where blockchain technology comes into play, because able to certify the existence, the creation date, the origin and the content of every document, contract, license or property.

A platform that deals with digital identity via blockchain is **Civic**, which attempts to give businesses and individuals the tools to control and protect their digital identities. Civic's structure identity platform bridges

---

[16] VeChain Foundation. (2017, December 05). VeChain Apotheosis: The Beginning. Retrieved June 13, 2020, from https://medium.com/@vechainofficial/vechain-apotheosis-the-beginning-d9f0fdbdc910

[17] RFID stands for "Radio-frequency Identification" and uses electromagnetic fields to automatically identify and track tags attached to objects. Near-field communication (NFC) is a set of communication protocols for communication between two electronic devices over a distance of 4 cm (1½ in) or less. NFC devices can act as electronic identity documents and are used for contactless payments. https://en.wikipedia.org/

[18] VeChain Foundation. (2017, October 30). VECHAIN INSIGHTS Vol.8. Retrieved June 13, 2020, from https://medium.com/@vechainofficial/vechain-insights-vol-8-c2988c8adcb

[19] Principles on identification for sustainable development: toward the digital age http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

the gap between the physical and digital storage of our private informations. In Civic these informations are private and can be accessed only by the owner, being identity data fully encrypted in the app on the users' device that can be accessed with biometrics. A fingerprint can be able to identify a person as the true owner of the data to any company, government or organization that is partner with Civic[20].

It is easy to understand how having a digital recognition system for every citizen can be a starting point towards the optimization of many other scenarios like, for example, voting. The digital vote could significantly reduce the risks associated with corruption and tempering of ballot papers. With blockchain, a digital vote would become a transaction, and as we have already seen, the consensus of the network does not allow for any double spending, thus eliminating the risk of votes falsification. The votes count becomes immediate and verifiable ensuring, among other things, a significant economic saving.

Nasdaq **eVoting** is a project, unveiled in 2016, that led to the creation of a platform based on blockchain to simplify voting processes. At the time, company's officials hoped to reduce both complexity and costs of organizing shareholder votes. Overall, the platform has successfully demonstrated how a blockchain could be used beyond transaction settlements[21].

2.2.4 Education

According to a report published in 2017 by the European Commission named "Blockchain in Education"[22], the attention is focused on the possibility of tracking, in a digitalized way, the knowledge and skills achieved by the students, thus designing a unique and immutable profile of the course of study of each student.

The Commission discusses various scenarios and addresses potential challenges, such as the recognition and transfer of credits, digital certifications, the multi-step recognition and students' payment transactions.

Despite the one of education being a fairly slow field in innovation, many important institutes all over the world have already started working towards the adoption of blockchain systems. In 2017, the MIT announced the issuance of certificates through an app called Blockchain Wallet, which allows the graduates to access a digital version of their diploma, prospecting potential employers and others[23].

Some practical examples of how blockchain is being implemented in the education system are:

---

[20] https://www.civic.com/blog/civic-is-redefining-digital-identity/

[21] Higgins, S. (2017, January 23). Nasdaq Declares Blockchain Voting Trial a 'Success'. Retrieved June 13, 2020, from https://www.coindesk.com/nasdaq-declares-blockchain-voting-trial-a-success

[22] Grech, A., & Camilleri, A. F. (2017). Blockchain in Education (A. Inamorato dos Santos, Ed.). Retrieved June 14, 2020, from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf

[23] Sundararajan, S. (2017, October 20). 100 Diplomas: MIT Issues Graduate Certificates on a Blockchain App. Retrieved June 14, 2020, from https://www.coindesk.com/100-diplomas-mit-issues-graduate-certificates-on-a-blockchain-app

- **Blockcerts,** which is a platform for creating and issuing blockchain-backed certificates. Creating academic transcripts and credentials on blockchain would allow companies to review the credibility of the documents and make sure that there are no falsified informations[24].
- **Appii,** on the other hand, uses blockchain to verify CV credentials. Verified achievements, qualifications and experiences will solve potential employers valuable time and money in the recruitment process. With blockchain-based CV verifications, candidates have higher chances of employability[25].
- **Odem** is a decentralized marketplace for educational products and services such as courses and resources. Using smart contacts, Odem connects professors and students where they can agree on specific courses that will helps improve students' education and bolster their academic background. Student can also use Odem tokens to pay for courses. In addition, Odem impacts the industry by creating "skill badges" for educators and students to show their level of experiences in certain areas[26].

2.2.5 Energy

According to a report published by PwC on blockchain opportunities for energy producers and consumers, blockchain technology appears capable of enabling a decentralized energy supply system.

Blockchain makes it possible for the energy network to be controlled by smart contracts based on rules designed to ensure that all energy and storage flows are automatically controlled to balance supply and demand. For example, when energy is generated more than needed, through smart contracts we could ensure that the energy in excess is delivered into storage automatically. Conversely, the energy hat has been stored could be deployed for use whenever the output is insufficient.

With a decentralized storage of all transaction data on the blockchain it'll be possible to keep a distributed and secure record of all energy flaws and business activities. Moreover, the ownership history of each certificate (for example, renewable power and emission allowances) could be recorded on the blockchain and customers could use cryptocurrencies to pay for the energy supplied[27].

Power Ledger is a global peer-to-peer, smart contracts based, energy distribution platform which enables customers and businesses to sell the surplus energy generated from rooftop solar panels. As for now Power Ledger in working in Australia, New Zealand, Asia, South Africa and many other countries. It allows to sell

[24] https://www.blockcerts.org/

[25] https://appii.io/

[26] https://odem.cloud/

[27] Blockchain – an opportunity for energy producers and ... (n.d.). Retrieved June 15, 2020, from https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf

surplus energy to your neighbors or whoever you want. Power Ledger allows you to perform energy transactions in real time between different users around the world, giving the community the opportunity to obtain energy self-sufficiency. Their goal is to make it easier and cheaper for people to "choose energy from renewable sources"[28].

The aforementioned applications are just some examples of the sectors where blockchain has the potential to bring a change. In general, the properties of its security, privacy and traceability make the blockchain itself the perfect tool to secure any type of transaction whether it's human-to-human or machine-to-machine. The blockchain has been especially identified to be well-suited in developing countries where trust is a major concern. Hence, the blockchain technology can be seen as an essential component of the Internet that was lacking in security and trust.

In the next chapter a deep analysis of the Bitcoin protocol will be provided to give an understanding of how monetary transactions work in a decentralized system.

[28] https://www.powerledger.io/

3 CHAPTER 3: THE ARCHETYPE OF CRYPTOCURRENCY – BITCOIN

3.1 WHAT IS CRYPTOCURRENCY?

Lately, cryptocurrencies have become a global phenomenon known to most people. Specifically, cryptocurrency is an internet-based medium of exchange that uses cryptographical functions to transmit value in a digital setting (i.e. conduct a financial transaction). Cryptocurrency leverage blockchain technology to gain decentralization, makes cryptocurrencies theoretically immune to a centralized control and other interferences, transparency and immutability.

Cryptocurrencies intended as a medium of exchange have been the first application to exploit the blockchain potential, creating a new paradigm in the world of the payment system. It is the first example of the Internet of value.

Internet is based on the TCP/IP protocol, where TCP stands for Transmission Control Protocol and IP for Internet Protocol. TCP/IP defines how data should be transmitted between two interconnected devices on the internet. When data are sent through the internet, they are always transmitted as a copy. But what happens when we want to transfer value?

A model where digital entities can be easily duplicated is not appropriate when adapted to a scenario where we want to transfer a real asset like money. Every object that is valuable should not be duplicated given that its value rests in its unicity. A situation where someone can transfer money as a copy is not conceivable, since it will allow that someone to spend it multiple times. What I have already described is known as the double-spending problem, a situation in which there exist more than a digital copy of something that should have been unique.

In a traditional model, double spending can be avoided thanks to a centralized entity such as a bank, which correctly updates the user's account. The DLT and blockchain are the first technologies that are capable of solving the double-spending problem in a decentralized way and the most famous example of this practice is Bitcoin, which will be discussed in detail in the following paragraph.

3.2 BITCOIN

"The Times 03/Jan/2009 Chancellor on brink of second bailout for bank" - the cryptocurrency's inventor embedded the hexadecimal code of the genesis block's coinbase with an encrypted Times headline from Jan 3rd, 2009, referencing the bailout of the United Kingdom's banks[29].

It is clear what was the goal of Satoshi Nakamoto - the still mysterious Bitcoin inventor or collective identified under this name. Obviously, the timing of this innovation isn't random at all. Bitcoin was both the

[29] Bitcoin turns ten on anniversary of "Genesis Block", https://cointelegraph.com/

solution and an indirect consequence of a crisis that was bringing the world to his knees. It arose to make obsolete that system which would have probably caused who knows how many more crisis in the years to come.
However, Satoshi Nakamoto's history starts a few months back. It was August 2008 when the domain *bitcoin.org* was registered. A couple of months later, for the first time ever this term appeared in a mailing list of a cryptography website[30] where a user under the pseudonym *Satoshi Nakamoto* claimed to have invented an electronic currency able of creating a monetary system needless of a fiduciary third party, and to have solved the most important problem in the context of electronic payments: the double spending. As a demonstration, Satoshi attached a document headed *Bitcoin: A peer-to-peer electronic cash system* where it was included a technical description of Bitcoin functionality[31].

In order to move forward with the analysis of Bitcoin, it is important to distinguish between its different meanings. That is, whenever we find the word *bitcoin* with the lowercase initial letter, we are referring to the cryptocurrency. Instead, if we find the word *Bitcoin* with the capital letter, we are referring to the open source protocol developed for the use of the cryptocurrency.
Bitcoin protocol is a cryptographic and pseudonymous - which is different from anonymous - structure, able to protect the user's identity and of facilitating the value exchange through a decentralized and disintermediated monetary paradigm.

Now, we can start to discuss the security element on which the entire protocol is based: cryptography.

3.3 ADDRESS, WALLET AND TRANSACTIONS

3.3.1 Asymmetric Cryptography

"Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents"[32]. In blockchain, cryptography is of particular importance. As we will see later on, the *addresses* on the blockchain are generated through a cryptographic system and the transactions will be authenticated through *digital signatures* - that is one of the most famous application of public-key cryptography.
Asymmetric cryptography is a process that uses a pair of related keys - one public key and one private key - to encrypt and decrypt a message and protect it from unauthorized access.

[30] *metzdowd.com*

[31] Bitcoin white paper, https://bitcoin.org/bitcoin.pdf

[32] Kaspersky. (2018, August 06). Cryptography Definition. Retrieved June 16, 2020, from https://usa.kaspersky.com/resource-center/definitions/what-is-cryptography

- A **private key** (also called *Master Seed)* is generated randomly and has to remain secret.
- A **public key** - derived from the private key - can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key.

Those keys are nothing more than extremely big numbers, usually represented in hexadecimal (0-9 to represent numbers from 0 to 9 and a-f to represent numbers from ten to fifteen).
The cryptographic algorithm on which Bitcoin protocol is based, in order to generate and make the key interact with each other, makes use of the Elliptic Curve algorithm - or, ECDSA (*Elliptic Curve Digital Signature Algorithm).*
In Bitcoin, for example, the private key corresponds to a number of 256 bit (in other words, a sequence of 256 ones and zeros). The biggest number that can be saved in 256 bits is 2^256. To give the idea, 2^256 = 10^78 and the number of atoms in the observable universe is approximately 10^80[33]. Generating two identical private keys, even if mathematically possible, is EXTREMELY unlikely.
To generate a public key starting from a private one[34] is actually very easy, but to invert this operation is practically impossible. Public Key encryption can be used in order to guarantee some properties like encryption, authentication and integrity in a hostile environment like Internet.
Now, to make an example: the sender uses the public key of the receiver to encrypt the message; the receiver is the only one that can decrypt the message using its private key. In this way sender and receiver can safely communicate without ever meeting. But, also in this method there is a fallacy: a third person could intercept the message and modify it, using the public key of the receiver; in this way, when the receiver gets the message, he/she cannot tell whether the message has been substituted. In order to solve this problem, in Bitcoin is made use of a function that has already been explained in the course of this work, the hash function. As we have said already, this function can be defined as a digital signature and is an extremely efficient method in order to verify the authenticity of a message and notice if it has been modified, because is that case the hash would have drastically changed.
Now that we have contextualized the importance of the hash function, we can discuss the characteristics of the Bitcoin protocol.

[33] Number of atoms in the universe - Wolfram: Alpha. (n.d.). Retrieved June 16, 2020, from https://www.wolframalpha.com/input/?i=number+of+atoms+in+the+universe

[34] The public key is generated from a private key through ECC (*Elliptic Curve Cryptography)*

3.3.2 Address

On a blockchain there are no users' profiles, but rather addresses. An address is where our bitcoins are virtually contained. Whenever we have to receive a payment, we provide our address to the person that has to send us bitcoins. The address is calculated starting from a public key. In fact, the entire process starts from the creation of a private key from an entropy[35]; from this private key we can generate, thanks to ECDSA algorithm, the corresponding public key and from this last one, it can be generated our bitcoin address.
In order to derive an address from the public key, different hash functions are applied (SHA-256, RIPEMD160 and BASE58CHECK) and the final result looks something like this: 35hK24tcLEWcgNA4JxpvbkNkoAcDGqQPsP[36]. As we can see, a Bitcoin address is an alphanumeric identification code composed of approximately 34 characters starting with 3 or 1.
We have said how the address does not actually contain cryptocurrencies. So where are our cryptocurrencies stored? In reality, nowhere. Blockchain is just a list of transactions, it doesn't exist the concept of currency as a tangible object that can be stored somewhere. Money is just an accounting item, and the final balance of an address is calculated after examining all the transactions involving that address.
A bitcoin address can be represented also as a QR code and it doesn't contain any informations about the owner. At present we mistakenly read or hear that Bitcoin allows for anonymity, but this is not entirely true. Bitcoin protocol, thanks to the blockchain technology, makes every transaction of the address traceable and transparent. What is not visible, however, is the holder of the address. This is why is safe to say that Bitcoin guarantees the pseudonym of the users, since every address holder can deliberately choose whether to associate to the address its name or a pseudonym, just like it works for email accounts.

3.3.3 Wallet

Contrary to common belief, crypto wallets do not store cryptocurrencies. Instead, they provide the essential tools to interact with a blockchain. It is properly a digital "keychain" that manages the private key and contains, likewise, the corresponding public keys. It is important to highlight that bitcoin are not located in wallets so, when a transaction takes place, BTC are not exchanged from a wallet to another. Instead, when making a transaction, what is registered on the wallet is the change of ownership occurred after the transaction. Additionally, each wallet keeps track of all the BTC owned, showing the total balance and simplifying the user experience.
When entering the cryptocurrency market, it is important to keep in mind that the underlying technology is the blockchain, which inevitably carries the concept of decentralization. Indeed, when a fiduciary third party is missing, to which we are used to refer whenever we have issues with our banking accounts, we have a

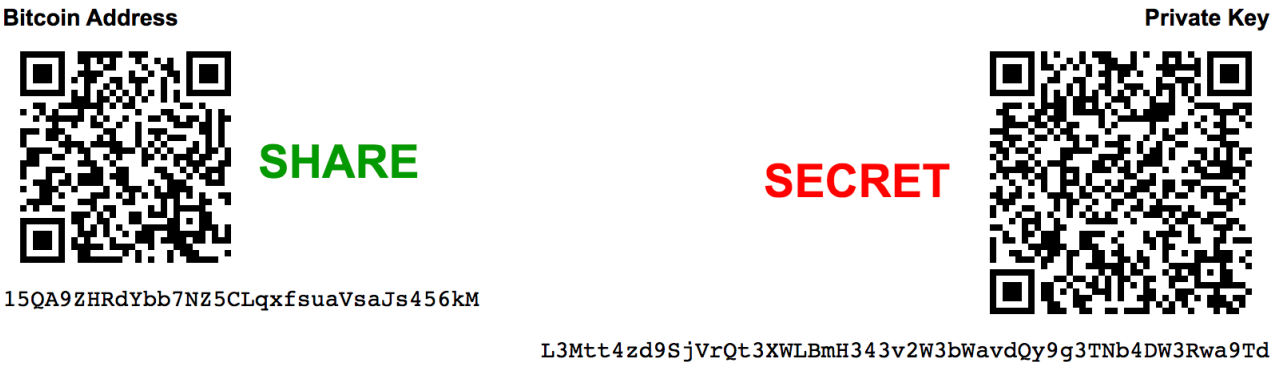
[35] "Entropy is a known measure of "randomness" of the system. On statistical level, entropy also measures the amount of information, that is needed to completely "describe" the system." https://medium.com/bitquery/bitcoin-and-ethereum-balances-and-its-entropy-c0e1254de29a

[36] This is the address with the highest number of bitcoins. https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

higher responsibility. Specifically, we won't find any “customer care” or “client support” to contact if we are facing any kind of issue. As a consequence, it is essential to carefully store our private keys. If those keys are lost so will be our funds or, if someone came to know our private key, he/she could, without any problem, gain access to our wallet and transfer money on its own wallet.
In order to avoid these events, we can distinguish between three different types of wallet: *software, hardware* or *paper.* Additionally, depending on the context in which these wallets are being used, we can distinguish two macro categories: *cold storage* and *hot storage.*

A **hot storage** wallet is in some way connected to the Internet, that is, our private keys were created and are currently stored on a machine connected to the Internet. On the contrary, a **cold storage** wallet refers to a wallet where our private keys never came into contact with Internet. A cold storage solution is extremely more secure, since is harder to steal something that has never been connected to the Internet. A **paper wallet** is the simplest form of cold storage. Is just your private key and address printed on a piece of paper, the security of the paper wallet lies in the security of the place where the piece of paper is hidden.

Figure 2.1 - example of paper wallet (www.bitaddress.org)



A **software wallet** is an application that can be downloaded on a computer or a smartphone. The private key is codified with a password and stored on the machine itself. Software wallets are usually chosen for their use friendliness, however, if the machine were to be compromised, the private key could be stolen.
A **hardware wallet** stores the private key in a device (hardware). It has great security benefits compared to a software wallet, since private keys are stored in a protected device from which they cannot be extracted. At the moment, hardware wallets represent the best compromise in terms of security and easiness of use.
Generally, the first time that a hardware or software wallet is being used, a list of words to memorize is communicated. This list is called "passphrase" and allows to restore the wallet in order to regain access. In this kind of wallets, called **wallet HD** (Hierarchical Deterministic) the passphrase is the starting point from where the private key is generated. The words that compose the passphrase represent the “randomness”.

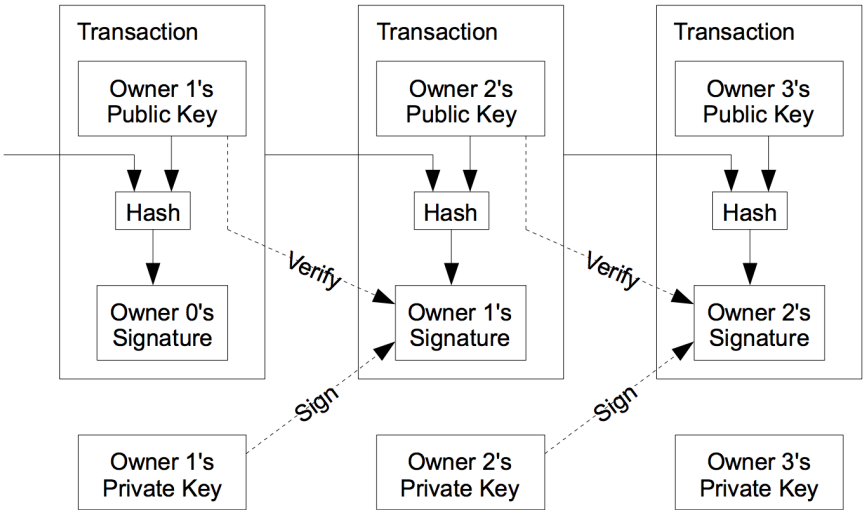
These wallets implement a system to derive the keys from a single starting point also known as “seed”. The seed allows the user to restore a wallet without any further informations. If a computer, a hard disk, or a hardware wallet were to be destroyed, it would be easy to restore private keys on another device by reinserting this seed.
Address and wallets are two of the fundamental components needed in order to do what bitcoin was created for, that is: decentralized transfers of value.

3.3.4 Transactions

Cryptocurrency transactions are one of the fundamental break points with respect to traditional payment systems. Bitcoin transactions rely on cryptography, and not on a fiduciary third party.
Satoshi Nakamoto assumed that in order to equally safeguard both parties of the exchange, that is to confirm the non-existence of a potential transaction, the only way was to be aware of all the transactions already occurred[37]. Hence, the need of a public network of users that could view and confirm the order of each transaction, so as to guarantee to the person that has to receive a payment that the sender is in possession of that amount of money.
At this point, in order to carry out a transaction we only need the address that identifies the wallet of the person that has to receive the payment. In our wallet will be stored our private key that serves to sign the transaction and provide a cryptographic proof of their origin. In this way, whoever wants to send bitcoins to someone else only has to digitally sign the hash of the previous transaction and add the public key of the receiver. After which, the transaction itself goes through the Bitcoin network and wait for the participants of the network (nodes) to validate the cryptographic signatures and confirm the transaction. At this point the transaction becomes irreversible, public and potentially anonymous (it is possible that the parties are only aware of the corresponding addresses).

[37] Bitcoin: a peer-to-peer electronic cash system https://bitcoin.org/bitcoin.pdf

Figure 2.2 Example of Transactions - Source: https://bitcoin.org/bitcoin.pdf



In order to be sent, every transaction need three basic elements:

- An **Input**, that is a reference to an output of a previous transaction. A transaction can contain multiple inputs and the sum of all the inputs give a total that represent your balance - that is, the added value of unspent previous transaction outputs are the coins you may claim. Additionally, a script component is included, which contains your signature and public key. The public key is used to verify your signature and prove that you are the address owner and are entitled to send that amount of coins.

- An **Output** is comprised of instructions for spending the coins. It is composed of two variables: the value in Satoshi of the transaction (Satoshi is a structural part of the Bitcoin cryptocurrency, which is one hundred millionth of bitcoin, so `1 Satoshi = 0.00000001 BTC`)[38] and the ScriptPubKey which is the second half of the script of reference (or address) to which send the amount of BTC. If `output > input`, the transaction will not take place, but if `input > output`, the difference will be donated as a commission to the miner that will validate the transaction on the blockchain.

- A **Proof of Work**, the consensus protocol used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to find the solution to a mathematical problem, complete transactions on the network and get rewarded.

[38] Satoshi https://it.bitcoinwiki.org/wiki/Pagina_principale

Now that Bitcoin transactions have been explained, we can return on the concept of Blockchain and explain more in details the anatomy of the blocks of a Blockchain applied to cryptocurrencies.
Each block is composed of two fundamental parts[39]:

- The **Block Header** which contains various informations such as:
  - The number of the block, which is the sequence number of the block added to the chain (the genesis block is associated with the number zero).
  - The version number of the software
  - The time in seconds since 1970–01–01 T00: 00 UTC, which is a timestamp in the block itself and the time is given in seconds since 1/1/1970.
  - The hash of the previous block
  - The root hash of the *Merkle tree*. This contains the hash of all the aggregated transactions present in a block.
  - The goal of the current difficulty, that is the elaboration time necessary in order to solve a mathematical problem in the mining operation.
  - The nonce, which guarantees that the data in the block are being used only once.

- The **Block Body** contains all the confirmed transactions. Constructing a block means validating the transactions. That is, the miner checks that the sender has enough money to spend and he can easily read this information from the blockchain.

It is important to mention that the first transactions that appears on each list of any block is called *coinbase.* This is added to the block by the miner that has solved that block first, that is the miner that has validated and confirmed the transaction first, through the activity called "Mining", which will be explained more extensively in the next section, together with a better definition of the PoW.

3.4 CONSENSUS IN A TRUSTLESS NETWORK: MINING

Computers and software are not perfect systems: they can get stuck, being hacked or even behave randomly. When we connect different computers together in a network, the uncertainty of the final outcome grows exponentially. In a blockchain there can be millions of nods who function independently, therefore is not possible to foresee how they will work. Given that in a permissionless blockchain it is not possible to trust any entity, how is it possible for a network to agree on a single status? How does a node decide to validate a certain transaction?

[39]Antonopoulos Andreas, "*Mastering Bitcoin: Programming the Open Blockchain*", 2017

The network has the goal to reach an ultimate decision on what has happened inside the blockchain through a process called *consensus*.

The consensus of blockchain is that all nodes maintain the same distributed ledger. In traditional software architecture, the consensus is hardly a problem because of the existence of the center server, hence the other nodes only need to be aligned with the server. Instead, in a distributed network such as blockchain, each node is both a host and a server, and it needs to exchange information with other nodes to reach a consensus. Sometimes some nodes will go offline, and there will also be some malicious nodes, which will seriously affect or destroy the process of consensus. Thus, an excellent consensus protocol can tolerate the occurrence of these phenomena and minimize the harm so as not to affect the final consensus result.

The consensus process involves several participants, each with its own role and responsibility. As we will see later on, the two principal actors in this process are the full-nodes and miners.

However, the achievement of consent in a decentralized and distributed system is very complex. This situation is clearly explained by the Byzantine Generals Problem.

3.4.1 Byzantine Generals Problem

In 1982 the mathematicians Leslie Lamport, Marshall Pease and Robert Shostak decided to use a metaphor to theorize one of the most famous dilemmas in distributed systems: The Byzantine Generals Problem[40].

As Mike Maloney explains in his recent documentary[41], the Byzantine Generals Problem can be summarized by asking how to make sure that multiple entities, separated by distance, will be in absolute agreement before an action is taken.

Before considering possible solutions to this, the problem hypothesizes a scenario such as:

"The generals must decide only whether to attack or retreat. Some generals may prefer to attack, while others prefer to retreat. The important thing is that every general agrees on a common decision" […] "The problem is complicated by the presence of treacherous generals who may not only cast a vote for a suboptimal strategy, they may do so selectively" […] "The problem is complicated further by the generals being physically separated and having to send their votes via messengers who may fail to deliver votes or may forge false votes"[42].

---

[40] Il problema dei generali Bizantini e la soluzione di Bitcoin. (2019, August 02). Retrieved June 16, 2020, from https://cryptonomist.ch/2019/08/04/problema-generali-bizantini-soluzione-bitcoin/

[41] From Bitcoin To Hedera Hashgraph (Documentary) Hidden Secrets of Money Episode 8 https://www.youtube.com/watch?v=SF362xxcfdk

[42] Byzantine fault. (2020, June 04). Retrieved June 16, 2020, from https://en.wikipedia.org/wiki/Byzantine_fault

So, given these conditions, can the army execute a strategy?

The solution to the problem relies on an algorithm that can guarantee the following conditions:

1. The loyal generals will decide upon the same action plan, and
2. A small number of traitors cannot make the loyal generals adopt a wrong plan.

The loyal generals will do what the algorithm says they should do, but the traitors may deviate as they wish. Moreover, the algorithm must guarantee that the loyal lieutenants not only reach an agreement, but they agree upon a reasonable plan.

Up until 2008 this problem had never found any plausible solution; it was Satoshi itself that towards the end of the year explained how his system is a solution not only to the double spending problem, but also to the Byzantine Generals one.

The center of the dilemma rests on communication: in fact, a general is able to communicate with another only through delivered messages. As a consequence, those messages could arrive late, be destroyed or manipulated. According to Satoshi, applying this problem in the blockchain context, each general represents a node in the network and the majority of the participants of the distributed network has to agree on and execute the same action. Once decided from one of the generals the time of the attack, this one will be considered valid from all, but since the network is not sudden, it can happen that two generals simultaneously announce two different times for the attack, with the result that different generals will receive different indications.

In order to solve this second problem, it is then used the Proof of Work, which is defined as the verification of a transaction. In fact, when a general receives a message, he/she has to solve an extremely difficult problem. The first general to solve this problem is in charge of communicating it to the other participants. Meanwhile, if someone was working on a different attack time, he/she will have to substitute it with the one just received since it will be considered as the valid one. Hence, the blockchain makes an aggregate of nodes in the same network to work together and manage in a synchronized way the network. As a consequence, the only way to reach the consensus in distributed systems is to have at least 50% plus 1 of honest nodes.

The nodes that actively participate in the consensus process are called *miners* and they perform an activity called *mining*.

3.4.2 Mining

Mining is a general concept and is not correlated to any blockchain in particular (even if it is usually associated with Bitcoin because it was the project that made use of it first). It can be seen as a process that allows the network to validate transactions, group them in blocks and add them to the blockchain. These operations allow the achievement of a distributed consensus and make the network secure.

Previously, I've said how the consensus is a continuous process in which miners and full nodes work in order to add new blocks to the blockchain and validate those blocks and the transactions. More in depth, a miner is responsible of, together with the nodes, verifying transactions and new blocks and spread them to the rest of the network. Choose the valid transactions, order them and store them in a block.

A full node is also responsible of verifying the transactions and blocks and in case of positive outcome spread them to the network. Hence, a full node also contributes to the security of the blockchain checking the validity of each transaction and block, so as to guarantee that the miners do not "cheat". For this reason, when we introduced the distinction between a full node and a light node, we said that a full node is the safest way to use the blockchain. This is because a full node will never accept a block or a transaction that does not meet the criteria.

If a miner creates an invalid block, the other nodes will deny it. When the block of a miner is added to the blockchain, the miner will be compensated for its work. In Bitcoin, this happens once a miner has verified 1 MB worth of bitcoin transactions. The 1 MB limit was set by Satoshi Nakamoto and, depending on how much data the transaction takes up, this limit can be as small as one transaction or several thousand. To sum up, in order for a miner to earn bitcoins, he need to meet two conditions:

- verify ~1MB of transactions, and
- be the first miner to find he solution to a numeric problem. Which is the process also known as Proof of Work.

So far, we have described the Proof of Work as a process to solve a difficult mathematical problem. In reality, no advanced math is involved. What they're doing is basically guesswork.

They are trying to be the first miner to come up with a 64-digit hexadecimal number (namely a hash) that is less than or equal to the target hash. Mining is the only way to release new cryptocurrency and as for May 2020, there are around 18.4 million bitcoins in circulation[43].

Every single one of those bitcoins, except the ones put in circulation by the genesis block, came into being because of miners. In the absence of miners, Bitcoin as a network would still exist, but there would never be any additional bitcoin. The network is programmed to cut the miners remunerations by 50% every four years, also known as an event called *halving.* For example, in 2016 a miner's remuneration was set at 12,5 BTC; today, after the halving that took place on May 11th 2020, miners remuneration is 6,25 BTC. According to the Bitcoin Protocol, the total number of bitcoins will be capped at 21 million[44]. However, because the rate of bitcoin mined is reduced over time, the final bitcoin won't be circulated until around the year 2140. But how does mining take place? What is the equipment needed?

[43] https://www.blockchain.com/charts/total-bitcoins?

[44] How does Bitcoin mining works? https://bitcoin.org/

Early on in bitcoin's history individuals have been able to compete for blocks with a regular at-home computer, but this is no longer the case. The difficulty of mining changes over time to ensure smooth functioning of the blockchain and its ability to process and verify transaction. If 100 miners are competing to solve the hash problem, it is more likely that they'll reach a solution faster than a scenario in which 10 miners are working on the same problem. For this reason, Bitcoin is designed to adjust the difficulty of mining every 2,016 blocks.

When the collective computing power working to mine for bitcoin increases, the difficulty level of mining also increases to keep blocks production at a stable rate. To get a sense of just how much computing power is involved in the mining process, when Bitcoin launched in 2009 the initial difficulty level was one. As of March 3rd 2020, it was more than 16 trillion[45].

In order to mine competitively, miners must now invest in powerful computer equipment in order to generate as many "nonces" [46] as possible, as fast as possible, to guess at the target hash. A nonce stands for "number only used once," and in Bitcoin mining is 32 bits in size—much smaller than the hash, which is 256 bits. The first miner whose nonce generates a hash that is less than or equal to the target hash, gets the reward for completing that block. Since the reward is paid to the winning miner, the probability that a participant will be the one to discover the solution is equal to the portion of the total mining power on the network. Participants with a small percentage of the mining power stand a small chance of discovering the next block on their own, not to mention that it would take a very long time as the difficulty going up makes things gradually worse.

The answer to this problem is mining pools. Mining pools are operated by third parties and coordinate groups of miners.

As of today, it is possible to carry out the mining activity in different ways:

- **Solo-mining** expects that the activity will be carried out by just one individual that tries to receive all the reward in BTC. As we have said, in order to carry this kind of activity is necessary to make a huge investment in terms of computational power, given the high level of competition. Thus, this activity does not guarantee a continuous cash flow, and it could pass a long time between the solution to one block and another. To raise the probability of receiving the reward, miners connect to a server called mining pool.
- **Mining Pool** is a server where miners connect and join their computational power to find blocks. The rewards are then split based on their individual contribute in terms of hash rate. For example, if in a mining pool there are three miners with computational power of miner1=xhash/s, miner2=2xhash/s

[45] https://btc.com/stats/diff

[46] A nonce refers to a number or value that can only be used once. Nonces are often used on authentication protocols and cryptographic hash functions. In the context of blockchain technology, a nonce refers to a pseudo-random number that is utilized as a counter during the process of mining. www.binance.vision

and miner3=3xhash/s, the total computational power = 6xhash/s. When the block has been solved, then miner1 gets 1/6, miner 2 gets 1/3 and miner3 gets 1/2 of the total reward. Typically, in mining pools there is a coordinator in charge of organizing the miners, make sure they use different values for the nonce so that they are not wasting hash power to create the same block. These coordinators, among other things, are responsible for splitting the rewards. There are several different methods in order to calculate the work done by each miner and split the reward accordingly.

- One of the most common payout schemes is *Pay-per-Share (PPS).* That means that the miner will receive a fixed amount for every share that has been submitted. The share is the hash used to keep track of the work of the miners. In PPS, the miner is rewarded whether or not the mining pool solves the block. The pool coordinator takes the risk so it is likely that a sizable fee will be charged.
- Another popular scheme is *Pay-Per-Last-N-Share (PPLNS).* This scheme only rewards miners when the pool successfully mines the block. As in the example above, when the pool finds a block it checks the last N amount of shares submitted, where N varies depending on the pool. To get rewarded, the amount of shares submitted is divided by N and the result is multiplied by the block reward (minus the operator's cut).

But, is the mechanism behind mining pools a threat for decentralization? What happens if someone gets the majority of the hashing power?

If a single entity can acquire 51% of the network's hash power, they can launch a 51% attack[47]. The attackers would be able to prevent the confirmations of new transactions, allowing them to stop payments between the users. They would also be able to double-spend coins reversing the transactions that were completed while they were in control of the network.

Mining pools could in theory increase the risk of a 51% attack, although it is very unlikely. This is because if the top four pool could collude to hijack the network the price of bitcoin would probably plummet as their action would undermine the system. This would not make much sense, since the consequence will be the loss in value of the coins they have acquired[48].

In the next section, a detailed description of two popular blockchain consensus protocols that are implemented to prevent double-spends will be provided.

[47] A group of miners controlling more than 50% of the network's computing power.

[48] Binance Academy. (2020, June 09). Mining Pools Explained. Retrieved June 16, 2020, from https://academy.binance.com/blockchain/mining-pools-explained

3.4.3 PoW (Proof of Work)

PoW is adopted by Bitcoin and other open source protocols. The Proof-of-Work comes in to make sure that users aren't spending money they don't have the right to spend.

As I have already anticipated, PoW selects one node to create a new block in each round of consensus by computational power competition. In the competition, the participating nodes need to solve a cryptographic puzzle. The node who first addresses the puzzle can have a right to create a new block. It is very difficult to solve a PoW puzzle. This "mathematical puzzle" is an issue that requires a lot of computational power to solve which is used to hash the block's data until a solution to a puzzle is found. Hashing the blocks data means passing it through a hashing function to generate a block hash. Previously in the discussion, we have defined the hash function as a "fingerprint" and is virtually impossible to reverse a block hash to get the input data. In this case, however, knowing an input it is trivial to confirm that the hash is correct and all you need to do is run the input through the function and check if the output matches.

In Proof of Work, we must provide data that matches certain conditions. The data is passed through the function to check if the conditions are met. If they are not, the data has to be changed slightly to get a different hash. This is why we defined this process more as a guessing game than a mathematical problem. Typically, the pieces of information of all the transactions, and some other data that are to be added, are taken and hashed all together. But since the dataset won't change, you need to add a piece of information that is variable, otherwise you would always get the same hash as output. This variable data is what we call a nonce. It's a number that you'll change with every attempt, so you're getting a different hash every time. And this is what we call mining.

As the network grows it faces more and more difficulties and nodes need to keep adjusting the value of nonce to get the correct answer. Although, the problem should not be too complicated because if it is, the block generation will take too much time. If this is the case transactions will be stuck without execution. On the other hand, the problem cannot be too easy because it would be prone to vulnerabilities, DoS attacks[49] and spam. The solution to the problem has to be easily checked. Otherwise, not all nodes are able to analyze if the calculations are correct and they will have to end up trusting the other nodes and violate one of the most important features of the Blockchain - transparency.

Summing up, mining is the process of gathering blockchain data and hashing it along with a nonce until you find a particular hash. If you find a hash that satisfies the conditions set out by the protocol, you get the right

[49] "In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled" https://en.wikipedia.org/wiki/Denial-of-service_attack

to broadcast the new block to the network. At this point, the other participants of the network update their blockchains to include the new block.

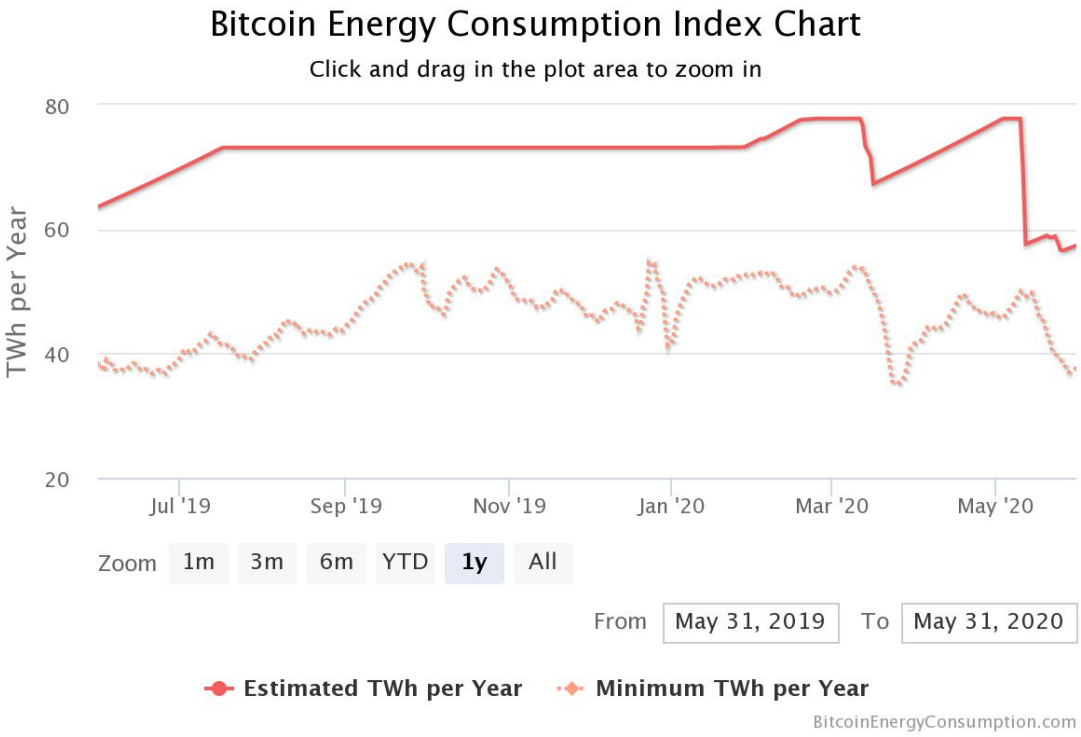
3.4.4 PoW: Pros and Cons

The main advantage of the Proof of Work is the strong guarantee of immutability. It is close to impossible to modify a transaction after it has been confirmed several times. A confirmation corresponds to the number of blocks added to the blockchain starting from the block that contains the transaction in question. Hence, to modify a block and the transaction in it, becomes harder and harder as blocks are added to the blockchain.

However, some would say that the PoW is not the best consensus mechanism, which has raised several controversies:

- **High energy consumption.** Bitcoin current estimated annual energy consumption is 57.39 TWh, which according to digiconomist.net, is comparable to the power consumption in Bangladesh. Many believe that this situation is not sustainable in the long term. The miners' "supercomputers" test millions of computations per second, and this is happening around the world. However, this enormous amount of computational power required is the reason why the PoW is so reliable as a consensus process. This is what guarantees the immutability of the blockchain.
  Bitcoin's biggest problem is perhaps not even its massive energy consumption, but the fact most mining facilities in Bitcoin's network are located in regions (primarily in China) that rely heavily on coal-based power.

Table 2.3 – Source: https://digiconomist.net/bitcoin-energy-consumption



- **Vulnerability to a 51% attack.** PoW is vulnerable to a "51% attack" meaning — in theory — nefarious miners could capture 51 percent of a network's computing power, gain what's termed "dominance" and manipulate the blockchain to their advantage. Thus, it could happen that the miner in question would be able to invert or modify some transactions (double spending) or block the confirmation of new transactions[50]. However, if a miner were to be successful in carrying out a 51% attack it would not be able to modify previous transactions, since it would have to recalculate the PoW of all the previous blocks while the other honest miners keep on working on the correct blockchain. Such an attack would require an enormous amount of resources. Hence, it would be more profitable to follow the rules of the blockchain.
  It is important to highlight that this argument is valid for a blockchain with a high level of hash rate as Bitcoin. A 51% attack on minor blockchains is possible.

- **Geographic discrimination and economies of scale.** At the moment the vast majority of Bitcoin miners are located in places where the cost of electricity and temperatures are very low, in order to save on electricity and cooling systems. Furthermore, economies of scale are used to negotiate convenient prices for both electricity and the necessary machines for mining. Often, this translates into a centralization of the mining process, concentrating the miners is certain geographic areas and make them share their computational power.

3.4.5 PoS (Proof of Stake)

Proof-of-Stake (PoS) algorithms are designed to overcome the disadvantages of PoW — in particular, high energy consumption. PoS, in its various permutations, is the most common alternative to PoW. Like PoW, it's also designed for a public blockchain.

PoS completely replaces the mining operation with an alternative approach involving a user's stake or ownership of virtual currency in the blockchain system. A white paper from Persistent Systems[51] offers a useful explanation:

"Instead of a user spending say $2000 buying mining equipment to engage in PoW algorithm and winning a mining reward, with PoS she can buy $2000 worth of cryptocurrency and use it as stake to buy proportionate block creation chances in the blockchain system by becoming a validator"

---

[50] S., J. (2019, December 24). Blockchain explained: How a 51% attack works. Retrieved June 16, 2020, from https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474

[51] Baliga, A., Dr. (2017, April). Understanding Blockchain Consensus Models. Retrieved June 16, 2020, from https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

The PoS algorithm pseudo-randomly selects validators for block creation, thereby there's no guarantee that the validator will be selected. In that sense, is like a lottery: the more you invest, the better your chances on being selected.

In PoS-mining, instead of the computational power, transaction confirmations are based on the number of tokens owned. In other words, the participants can "stake" their tokens (which only means to freeze them temporarily until the process is over) in order to get the right to confirm a block's transactions (become a validator) in return, and ultimately receive a reward. Therefore, the creator of a new block is chosen in advance based on a combination of different parameters such as the number of tokens (stake) or the amount of time that validator has been in possess of those tokens. For example, a validator that owns 10% of the total tokens, on average gets the right to create a new block 10% of the times.

Compared to the PoW, PoS is more efficient since complex calculations are not necessary. PoS supporters state that is has the following advantages:

- **Attacks are more expensive.** PoS is theoretically vulnerable to a 51% attack. But, in this case, a malicious miner will not need 51% of the hash rate, but 51% of the total tokens. However, if a participant would want to buy 51% of the total tokens, the market will react with a rapid increase in the price of the tokens. Moreover, who owns a considerable big amount of tokes will be less incentivized to attack the system, since it will destroy the trust in the blockchain and, as a consequence, the tokens value.

- **Affordable.** Given the absence of electricity and hardware costs, everyone is able to join the network reducing the centralization of the systems based on PoW.

- **Loyalty.** Miners are incentivized to stick with a certain blockchain. If a validator would want to participate in PoS on another blockchain, it will be obliged to change the tokens owned. In PoW, instead, if the currency that is being mined is no more profitable, miners can simply change blockchain.

In conclusion, there are many other consensus protocols other than PoW and PoS. Consensus models used by popular blockchain platforms today are largely driven by the type of applications the platform expects to cater to and the threats it envisages to the integrity of the chain. Typically, the permissionless platforms are achieving robust consensus among very high number of untrusted peers using computational or memory complexity while sacrificing transaction finality and throughput. On the other hand, the permissioned, consortium blockchains are opting for a less scalable but much higher throughout model that ensures faster transaction finality. So, when looking at blockchain to solve a business problem, it is important to look at the scale of the intended network, the relationship between participants and other aspects such as the performance and confidentiality before determining the right consensus model.

In the dynamic world of cryptocurrencies, as time passes, it could happen that a participant may notice the need to make some improvements to the network of that specific cryptocurrency. Technically speaking, it is often the case that some updates to the original code of a protocol are necessary. In the case where this type of proposal is successful, the modification of the original code is defined as *fork.*

3.4.6 Soft Forks and Hard Forks

As any software needs constant updates to fix issues or increase performance, in the crypto context these updates are defined as forks. There are two types of fork in crypto: soft forks and hard forks. Both kinds of forks fundamentally change how the protocol of a cryptocurrency works.

A **Soft Fork** is a change in a protocol that is backward-compatible. This means that nodes that are not updated can still process transactions and create new blocks in the blockchain, as long as they don't violate the new protocol's rules. Soft Forks are in general an optimization of the existing protocol.

To make an example, we take under exam the Bitcoin case. Bitcoin's fork happened in 2017 and is called Bitcoin Cash. We know that Bitcoin is not only the first cryptocurrency ever created, but as of today is also the most widely used. We can safely say, however, that Bitcoin has some flaws itself, such as the scalability. Due to the limited size of blocks (1MB), transactions elaboration times are much longer compared to other protocols, this decreases significantly the number of transactions that the network is able to process (4/7 transactions per second). As a consequence of this, in 2017 the time passing between a transaction an another had become a question of days, which would have made impossible for someone to pay, for example, a meal with Bitcoin. To face this issue, the Bitcoin community decided to suggest a new protocol able to redefine the block size from 1MB to 2MB. This new protocol was named SegWit2x. Before the SegWit2x proposal came about, there was Segregated Witness (SegWit) – a soft fork proposed in 2015 by a developer named Pieter Wuille[52], which aimed to address bitcoin's scalability problem.

In short, the mechanism of the Segregated Witness allowed data to be stored differently across blocks with the goal to increase the overall transaction capacity. SegWit only modified the structure of the block adding a new element called "witness", which contains the necessary informations to validate transactions (such as the digital signature) freeing up space in the block.

On the other hand, SegWit2x was a hard fork proposal. A **Hard Fork** is a "change in a cryptocurrency protocol which is incompatible with the previous versions, meaning that nodes that don't update to the new version won't be able to process transactions or push new blocks to the blockchain"[53]. Hard Forks can be used to create a new independent protocol or blockchain. However, as soon as SegWit2x was implemented,

[52] Reiff, N. (2020, January 29). What Is SegWit2x? Retrieved June 16, 2020, from https://www.investopedia.com/tech/what-segwit2x/

[53] Hards Forks and Soft Forks - Binance Academy. https://academy.binance.com/blockchain/hard-forks-and-soft-forks

it didn't seem like the problem had been completely solved. For this reason, it became necessary to implement Bitcoin Cash, which would have increased the blocks size from 2MB to 8MB. The result is a complete new blockchain and cryptocurrency, BTH. Bitcoin Cash is able to process transactions more quickly compared to the Bitcoin network, meaning that wait times are shorter and transaction processing fees tend to be lower. However, with the faster transaction verification time comes downsides as well. One potential issue with the larger block size associated with BCH is that security could be compromised relative to the Bitcoin network.

One of the consequences of a "division" in the blockchain is the sharing of the transaction history before the hard fork. This means that after a fork, the user will own the same quantity of tokens on both the blockchains.

It is clear by now how Bitcoin is the first decentralized cryptocurrency ever created, but it is not the only one. In fact, there are more than 2.000 cryptocurrencies in circulation and in the next paragraph I will make an analysis of the most interesting ones.

3.5 ALTCOINS

Altcoin is a generic term that refers to all the cryptocurrencies that have been created after Bitcoin. Some are similar to Bitcoin and some others are completely different under the blockchain structure, protocols and so on. In this paragraph I will analyze some of the best-known cryptocurrencies, divided according to the sector of application, referring to a recent scenario.

3.5.1 Ripple (XRP)

Ripple is a peer-to-peer protocol created in 2012 by Ripple Labs to facilitate the transfer of money on a global scale. It was designed primarily for banks and financial institutions and it is defined by Ripple itself as "the most advanced blockchain technology for global payments". XRP is the native digital asset on the XRP Ledger which is a permissionless and decentralized blockchain able to settle transactions in 3-5 seconds.

Within Ripple principal partnerships we can find American Express, Santander, Deloitte, UBS and UniCredit.

Ripple aims to solve one of the major concerns that banks and financial institutions have to face: global money transfer, especially transboundary payments. The process of transferring money between international banks it usually takes days and is followed by high transaction costs. This scenario is in stark contrast with a world where informations travel instantly all around the world thanks to the internet.

This is why Ripple created a service network named RippleNet. This network has the goal to interconnect banks and financial institutions and drastically reduce the time and costs of those kind of operations, becoming, as a matter of fact, a valid alternative solution to the Swift circuit.

XRP is designed to be used mainly by banks in reconciling their accounts, and not for users who make normal money transfers. For instance, it can be used for exchanges in dollars or in euros and to send money around the globe in seconds, allowing banks and financial institutions to reach new markets.

XRP is one of the non-minable cryptocurrencies, that means that all the tokens have been generated at the same time the ledger was created. XRP has a maximum quantity of 100 billion of units and every month 1 billion XRP are released, used to extend the adoption of its services.

Ripple exploits a public distributed ledger where all the informations relative to value movements are recorded. The distributed consensus is achieved through a consensus algorithm called RPCA (Ripple Protocol Consensus Algorithm) which employs groups of nodes considered honest by the network (UNL, Unique Node List). At least 80% of the nodes in the UNL has to judge the transaction as valid in order to be added to the ledger. This algorithm is very efficient and is able to generate a new ledger status every 3-5 seconds.

XRP ledger is connected to the reality thanks to **Gateway.** XRP Ledger Gateways are businesses that provide a way for money and other forms of value to move in and out of the XRP Ledger network.

Gateways can be banks, money service businesses, currency exchanges, or any other financial institution.

Gateway are also responsible of making sure that the rules are respected and to report to the authorities any suspicious behavior.

3.5.2 Ethereum (ETC)

Launched in 2015, Ethereum is blockchain-based, decentralized software platform used for its own cryptocurrency, ether. The Ethereum blockchain, differently from Bitcoin, is programmable. This means that people can build on the blockchain to create products and services. Thanks to the decentralized property of the blockchain technology, the software people can build on ethereum are called Decentralized Applications (DApps). DApps nature and potentials have inspired the idea and desire for a crusade towards Decentralized Finance (DeFi), which aims to transform the current financial system into a more transparent and trustworthy one.

Ethereum digital currency, the ether, works similarly to bitcoin but was created for an entirely different purpose. Instead of being used to transfer value, it was designed with the intention of “fueling” the Ethereum network.

On the Ethereum blockchain, the ether was created as a form of payment to fuel the ethereum network, in order to incentivize people to host and maintain the data on the blockchain. Anyone who wants to build a software application on the Ethereum network, has to pay for the computing power using ether.

The amount of ether required is determined by a system known as **Gas.** This system "considers the bandwidth and space requirements, as well as the computational difficulty of each transaction to calculate the amount of fees it would take to complete"[54]. The term "Gas" serves to differentiate the cost of performing a transaction on the Ethereum network from the actual value of the ether currency. When executing transactions on Ethereum we will see prices denoted in *gwei,* which is the most common unit of ether reflected in gas prices[55].

When initiating a transaction on the Ethereum network, you will be able to choose what is called a "gas limit", that is the amount of ether you are willing to spend to complete the transaction. The higher the gas price the faster the transaction will be processed. In the case where there's not enough ether to complete the transaction, you will receive an "insufficient funds for gas" notification or similar.

Currently, transactions of Ethereum are completed by miners via a Proof-of-Work protocol, processing and validating transactions in exchange for ether. So, using the Gas system, miners or nodes are able to set minimum amounts of gas prices that they are willing to accept to process transactions.

To better understand the Ethereum network I will break it down in three layers:

1. The base layer is the one where the network of nodes process, validate and broadcast transaction to the Ethereum network. As these nodes perform the computational work required to process transactions in data, they are rewarded with ether dictated by the gas prices we discussed earlier. These rewards incentivize the nodes to run and maintain the network.

2. On top of this hardware layer, there is a software layer. This software layer supports programming languages like Solidity, Viper[56] and more. These computer languages are the tools by which developers write the so-called *smart contracts* on the blockchain. In the previous chapter, I have discussed how smart contracts are basically lines of codes that dictate the terms of a contract and control its execution. Their unique ability rests on the fact that smart contracts are able to authorize transactions and check that the terms of the contract are being respected in a decentralized way, that is, without the need of a central authority.

[54] Nagritech.com. https://nagritech.com/

[55] Gwei = 1e9 wei, Ether = 1e18 wei

[56] Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum.
Viper is a contract-oriented, pythonic programming language that targets the Ethereum Virtual Machine (EVM).

3. The hardware layer and the software layer combined basically create a decentralized supercomputer known as the Ethereum Virtual Machine (EVM)[57]. The general idea of its role in the ecosystem is to improve the flexibility of the software and ensure separation of each software host in each software application. The application layer is where developers can build and launch DApps. There are several different DApps categories including games, exchanges, identity, health, property and more.

According to Vitalik Buterin, there are three types of applications on top of Ethereum. Firstly, we find financial applications, allowing users to manage and enter into contracts in a more powerful way. This application involves financial derivatives, hedging contracts, savings wallets, wills and more. The second category is semi-financial applications, which is a good combination of money involvement and non-monetary sides where financial resources are involved but they are tied to a non-monetary outcome; Buterin gives the example of "self-enforcing bounties for solutions to computational problems". Finally, there are non-financial applications that include voting and any other sort of decentralized governance of an organization that requires the democratic participation of its overseeing members.

Another smart contracts platform is **EOS**, which is conceptually similar to Ethereum but uses a different consensus protocol which is variation of the Proof of Stake called Delegated Proof of Stake. In this model there are no miners but 21 block producers, elected by owners of EOS tokens and remunerated with EOS. We can see the DPoS as a representative democracy. The block producers are constantly elected, and this system allows for an extremely quick generation of blocks.

NEO is a platform for the creation of DApps and is defined as a distributed network for smart economy, which is an ecosystem that integrates digital assets, digital identities and smart contracts. NEO provides a solution for the digitalization and management of physical goods in a decentralized way, allowing the creation of a real digital financial system connected to the real world.

3.5.3 Litecoin (LTC)

Litecoin was launched in 2011 by Charlie Lee, and one of the fist cryptocurrencies to follow bitcoin's footsteps. Litecoin was created with the intention to improve some aspects of Bitcoin, , in particular the one of making value transfers faster and cheaper. However, Litecoin is not to be seen as a Bitcoin's opponent, but more as a complementary network, more suitable for everyday payments and to shops and merchants. Other than developers, there are a growing number of merchants who accept Litecoin. As of Jun. 5, 2020, Litecoin is the seventh-largest cryptocurrency in the world with a market capitalization of $3.0 billion and token value of $47.60[58].

[57] In computing, virtual machines or VMS are emulations of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. https://en.wikipedia.org/wiki/Virtual_machine

[58] CoinMarketCap. https://coinmarketcap.com/currencies/litecoin/historical-data/?start=20181002&end=20191002

3.5.4 Tether (USDT)

Tether is one of the first and most popular **stable coin**. Stable coins are those kinds of cryptocurrencies that fix their market value to reduce volatility. Tether and other stablecoins attempt to smooth price fluctuations with the aim of attracting more users.

Launched in 2014, Tether describes itself as "a blockchain-enabled platform designed to facilitate the use of fiat currencies in a digital manner".[59]

This cryptocurrency is based on the dollar value, so 1 USDT is always equal to $1. On Jun. 5, 2020, Tether was the third-largest cryptocurrency by market capitalization with a total value of $9.2 billion and a token value of $1.01.[60]

Money in the digital form includes both virtual currencies – which are regulated and issued by a central entity – and cryptocurrencies – which, on the other hand, are part of a decentralized and distributed system.

The growing popularity of cryptocurrency has led to a revolution in the digital currency industry. As of today, a lot of big enterprises without a cryptocurrency background, have already created or are in process of investing resources to develop their own digital currency.

Cheaper and faster transactions are more likely to attract a big number of users, which will make the retail payment segment very much exposed to this new scenario.

Even if Bitcoin is the most famous and widely used cryptocurrency, it is true that on a global scale, cryptocurrencies are not well implemented in the everyday routine. However, the fact that tech giants such as Facebook, Telegram, Amazon and so on, are planning to adopt a digital currency could have a huge impact for our national markets and the world economy. The size of these technological companies would allow them to reach a very large scale, succeeding where cryptocurrencies have failed.[61]

Moreover, with the launch of digital currencies there exist another very profitable objective, that is the market of digital identity. With the digitalization of the economy, digital identity is the base for online and mobile interactions which allows to access banking and other sets of services.

---

[59] Tether. "FAQs. https://tether.to/faqs/ "

[60] CoinMarketCap. https://coinmarketcap.com/currencies/tether/

[61] Bilotta, N., & Botti, F. (2019, November 22). Libra and the Others: The Future of Digital Money. Retrieved June 07, 2020, from https://www.iai.it/sites/default/files/iaip1922.pdf

CONCLUSION

While the entire blockchain and cryptocurrency sector continues to grow and mature, we are also witnessing a "settlement" of its logic and dynamics. The companies whose products and services can have a real impact, in fact, continue to grow and consolidate their position on the market. At the same time other realities, in particular all the companies that have only tried to ride the growth of this technology for mere marketing, are starting to disappear from the radars, giving way to more useful products and solutions.

The process is just beginning, it will take time. When the sector grows further, however, the advantages of technology may be important not only for the companies that implement it, but also for individuals and businesses that use the services daily. Transparency, security, speed, disintermediation and a low transaction cost are all potential benefits of blockchain and cryptocurrency implementations in the contemporary social and entrepreneurial fabric.

The Estonia case is an evident example of all the advantages that are already evident in the adoption of the blockchain technology. In 2005 Estonia introduced the digital identity and since then has done nothing but add services to an electronic card that all citizens had. It is a credit card, with a sim inside, which can be connected to the bank account for telephone top-ups and payments and it can also be inserted into the phone as any SIM card and to make calls. Medical prescriptions and public administration services may be requested. All the informations about the Estonian ID that the government needs to allow the citizen to vote in the elections are stored in this card. It allows citizens to make a tax return, change residence, and - in these coronavirus emergency times - even register a new birth. The only times that the Estonian government explicitly requires a citizen to be physically present is when they have to do ID, because fingerprints are taken, and then when they get married, divorce and when they sell their house[62]. Everything else is digital.

Differently from other countries, Estonia has built over the years a solid digital government infrastructure that allows citizens to do almost anything online, avoiding physical contact.

Speaking of social advantages, Estonia is the only one in Europe who could be considered truly prepared to face the pandemic. Its citizens are those who, according to various surveys, suffer least from the sensations that we are all experiencing like panic, anxiety, fear and doubt.

This is because, after the lockdown announcement, they have launched a **hackathon**, that is, a competition of ideas to finance start-ups capable of responding to the crisis and in these days an accelerator will be opened with the support of the European Commission[63].

---

[62] Romano, B. (2017, August 25). Estonia, il sogno di un Paese tutto digitale. Retrieved June 17, 2020, from https://www.ilsole24ore.com/art/estonia-sogno-un-paese-tutto-digitale-AEp8d4GC

[63] Balena, C. (2020, March 27). Ecco perché l'Estonia era l'unico paese preparato al coronavirus . Retrieved June 17, 2020, from https://www.fortuneita.com/2020/03/26/ecco-perche-lestonia-era-lunico-paese-preparato-al-coronavirus/

Blockchain is the technology that has allowed this great step forward thanks to its potential to blindly trust data like never before. Identity and digital signature allow companies to set up and manage their practices quickly. Citizens can use protocol offices, document certification, public registers, and manage their personal data in faster, more reliable and safer ways.

Blockchain not only goes beyond Bitcoin and cryptocurrencies thanks to which it became well-known, but, as a matter of fact, it goes beyond its technology itself. Blockchain has the potential to influence every aspect of the global economy and introduce an entirely new set of possibilities across society. It is a real paradigm change.

[ANNEX.1] REFERENCES

Antonopoulos, A. M. (2018). *Mastering bitcoin: Programming the open blockchain*. Beijing ; Boston ; Farnham ; Sebastopol ; Tokyo: O'Reilly.

Comandini, G. L. (2020). *Da zero alla luna: Quando, come, perchè la Blockchain sta cambiando il mondo*. Palermo: Dario Flaccovio.

Chiap, G., Ranalli, J., & Bianchi, R. (2019). *Blockchain: Tecnologia e applicazioni per il business*. Milano: Editore Ulrico Hoepli.

Garavaglia, R. (2018). *Tutto su blockchain: Capire la tecnologia e le nuove opportunità*. Milano: Hoepli.

Zhang, S., & Lee, J. (2019, August 12). Analysis of the main consensus protocols of blockchain. Retrieved June 18, 2020, from www.sciencedirect.com

Miraz, M. H., & Ali, M. (2018, January 1). Applications of Blockchain Technology beyond Cryptocurrency. Vol. 2, No. 1, 2018

Sadhya, V., & Sadhya, H. (2018). Barriers to Adoption of Blockchain Technology.

Lamport, L., Shostak, R., & Pease, M. (n.d.). The Byzantine General Problem. *4*(July 1982), 382-401.

Ecco come la blockchain cambierà il modo di fare business ... (n.d.). Retrieved June 18, 2020, from https://www.ilsole24ore.com/art/ecco-come-blockchain-cambiera-modo-fare-business-le-aziende-AEtn1GfG

Buterin, V. (n.d.). Ethereum Whitepaper | Ethereum.org. Retrieved June 18, 2020, from https://ethereum.org/whitepaper/

Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved June 18, 2020, from https://bitcoin.org/bitcoin.pdf

Report: Blockchain banking in Italia e nel mondo. (2020, May 28). Retrieved June 17, 2020, from https://actafintech.com/2020/04/01/report-blockchain-banking-italia-mondo/

How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric. Retrieved from https://www.hyperledger.org/learn/publications/walmart-case-study

Principles on identification for sustainable development: toward the digital age http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

Grech, A., & Camilleri, A. F. (2017). Blockchain in Education (A. Inamorato dos Santos, Ed.). Retrieved June 14, 2020, from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf

Bilotta, N., & Botti, F. (2019, November 22). Libra and the Others: The Future of Digital Money. Retrieved June 07, 2020, from https://www.iai.it/sites/default/files/iaip1922.pdf