UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea Magistrale o Specialistica in International Economics and Commerce

Security Token Offering: Enterprise introduction to Blockchain and funding through STOs

Security Token Offering: Introduzione aziendale alla Blockchain
e funzionamento delle raccolte fondi tramite la procedura delle STO

Relatore: Chiar.mo
Prof. Caterina Lucarelli

Tesi di Laurea di:
Giorgia Bonacci

Anno Accademico 2021 – 2022

INDEX

Introduction

Over the years, society as we know it, has changed and is constantly evolving. Let us cast our minds, or imaginations, back to when the Geneva Research Centre launched the first website online in August 1991. It certainly must have been quite an impactful step for those who were catapulted into the reality of the Internet in those years. Gradually, people began to understand its usefulness and to have computers available in companies. Thanks to adaptation, today we find more than a billion websites and almost 4 billion users on the Internet. It is possible to say that the internet, thanks to its services, has revolutionised the way we live immensely. Today we are again faced with a change, an innovative technology that could fundamentally change human interactions: the Blockchain.

But what is it that drives society to innovate? Probably the need to solve the new problems that arise over time. Progress seen from the inside walks slowly, on a day-to-day basis we may not even notice it but if we look back the difference is clearly visible. Just as in the 1990s there was the challenge of understanding how internet applications could help us, with supporters and sceptics alike, today the focus is on blockchain technology. The problem that this technology tries to solve are problems that arose over time in the traditional internet applications: transparency, traceability and above all the problem of trust. To give a brief introduction to the technology let us jump back to 1400 AD and go to Micronesia to an island called Yap. On the island of Yap there was a need for an early form of currency and one

day during an expedition to a neighboring island the inhabitants found a rock not found on their island and decided to use it as a form of currency. They soon realised that heavier rocks were difficult to transport and could be stolen if left unattended. As a solution, each inhabitant began to keep a register where the ownership of each stone was noted. This register was updated by everyone at the time of a transaction so it would be possible for anyone to verify that an individual was in possession of the 'money' they wanted to spend and could not spend it twice because the information could be controlled. This decentralised system posed a solution to the problem of trust, it works exactly like the blockchain but in a primitive form. The blockchain was brought to attention in 2008 by Satoshi Nakamoto with the introduction of Bitcoin. Since then, there have been advances in the knowledge of the potential of the technology in various areas. One in particular, that will be covered in this text is the process of business funding by issuing tokens on blockchain. This process is called Security Token Offering (STO). However, to get to talking about STO, it is essential to have an introduction to what the technology is, how it works and what the main protocols are.

The first chapter will deal with the technology in general, where the functions and principles will be explained, as well as the types and levels of decentralisation. This is followed by the second chapter which talks about consensus algorithms and the two main protocols that will be covered in the paper: Bitcoin and Ethereum.

Then in the third chapter I tried to give a general overview of the applications of the technology in concrete terms, starting with a multitude of possible application sectors, concentrating on the financial sector immediately afterwards, and finally taking a look at a highly relevant topic; that of legislation.

Before arriving at the capital raising concept, I thought it was appropriate to have a sizeable comprehensive picture of the blockchain system. This way, one has the necessary tools to be able to understand the advantages but also the disadvantages that this technology has in certain situations. The ultimate goal of having a complete picture is, in fact to be able to understand the functioning of the protocols and, in particular to be oriented as far as fundraising is concerned about knowing the potential facets and being aware of the risks in order to be able to prevent them, such as having a clear understanding of the regulatory framework on which one is going to operate. In the fourth chapter, where the essential tools of capital raising, the tokens, are introduced, reference is also made to two other modes of fundraising, Initial Coin Offering and Initial Exchange Offering. Finally, in the last chapter, the fifth, the focus will be on the functioning of Security Token Offering (STO), the peculiarities of tokens and the types of tokens with a look again at legislations worldwide referencing STO in particular.

Chapter 1. The Blockchain

1.1 Blockchain enabling concepts

The blockchain is essentially a public ledger[1] with potential as a worldwide, decentralized record for the registration, inventory, and transfer of all assets—not just finances, but property and intangible assets such as votes, software, health data, and ideas.[2]

As the name suggest us, we can picture it by imagining an indefinite number of blocks linked together, and these links cause the chain to form. The blocks must be filled until the limit of 1 MB[3] with mostly information and transaction. Blockchain is a ledger distributed and managed by a network of computers, each of which has a copy of it. As Casey and Wong argue, since data is always updated simultaneously as it changes, it is possible to avoid those difficult processes between internal records that are used to do the same thing but with a real possibility of error. [4] The structure is made up of blocks connected to each other, each block contains several transactions, and each of them is validated by the computer network, in fact, the

[1] At this stage 'Ledger' indicates the literal meaning of the word. In the following sections, it will have a technical reference.
[2] Swan Melanie, Blockchain- Blueprint for a New Economy, 2015 pag. 2
[3] Nguyen C. T. *et al.*: Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks 85731
[4] Casey Michael and Wong, Global Supply Chains Are About to Get Better, Thanks to Blockchain, Harvard business Review, 2017

addition of each new block must pass through the consent of the computers (which act as nodes) based on a precise protocol.

Figure 1.1 The chain of blocks

Source: our processing

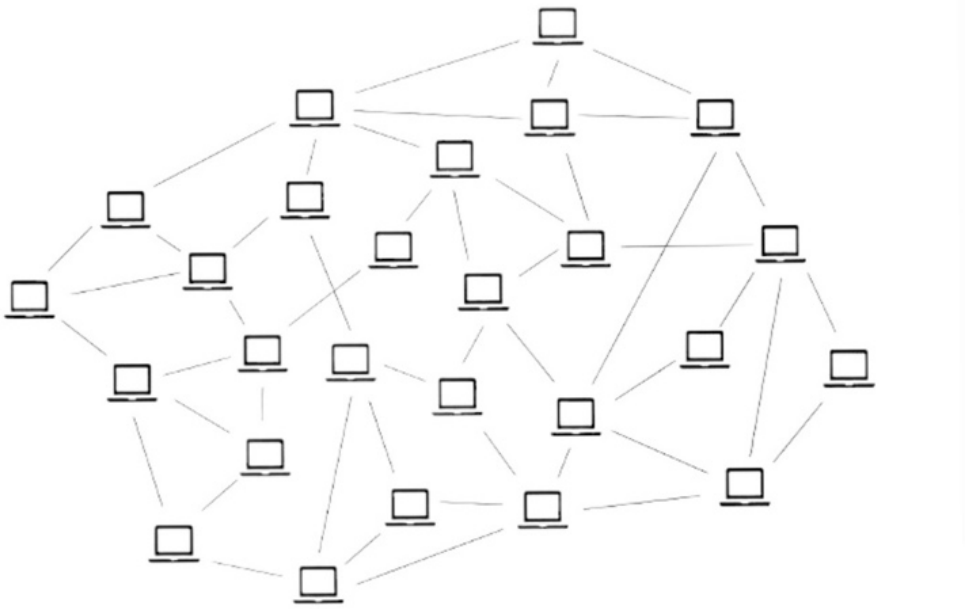
The protocol then manages the nodes' function and decides *whether a specific operation, such as a given payment, should be permitted or not*[5].

Each node of the chain is physically constituted by a server through which each participant has access to the blockchain and sees, controls, and approves transactions. Servers represent every single participant in the blockchain, and since it is decentralised there is no central server to which all others connect, but all individual clients connect to each other and form the network. Each node owns and manages a copy of the transactions that occurred in that blockchain, and when they are connected, they participate in the processing of transactions. Each time the addition of a new block is authorised, each node updates its copy, and in this way, that data will be hardly editable once it has been entered and validated. As Crosby et al. confirm, if an existing block were to be modified, this modification would need the consent of the entire chain to be made since the latter is made up of blocks,

[5] Pilkington M., Blockchain Technology: Principles and Applications, 2016

and it is assumed that the transaction had already been verified and confirmed by the different members[6]. Transactions in the blockchain cannot be traced back to an individual because privacy is provided by numeric alpha codes instead of explicit identifiers, as well as all other information thanks to encryption. *The data encryption and coding in a blockchain improve transparency, efficiency and trust in information sharing*[7].

Figure 1.2 Decentralised network



Source: Academy moralis, Exploring Parity Technologies' Substrate, 2021

[6] Crosby et al., Blockchain Technology: Beyond Bitcoin, 2016
[7] Misra, P., "5 Ways blockchain technology will change the way we do business", 2018

This figure represents the decentralized network of nodes; each computer represents a node/server, and each of them holds a copy of the registry.

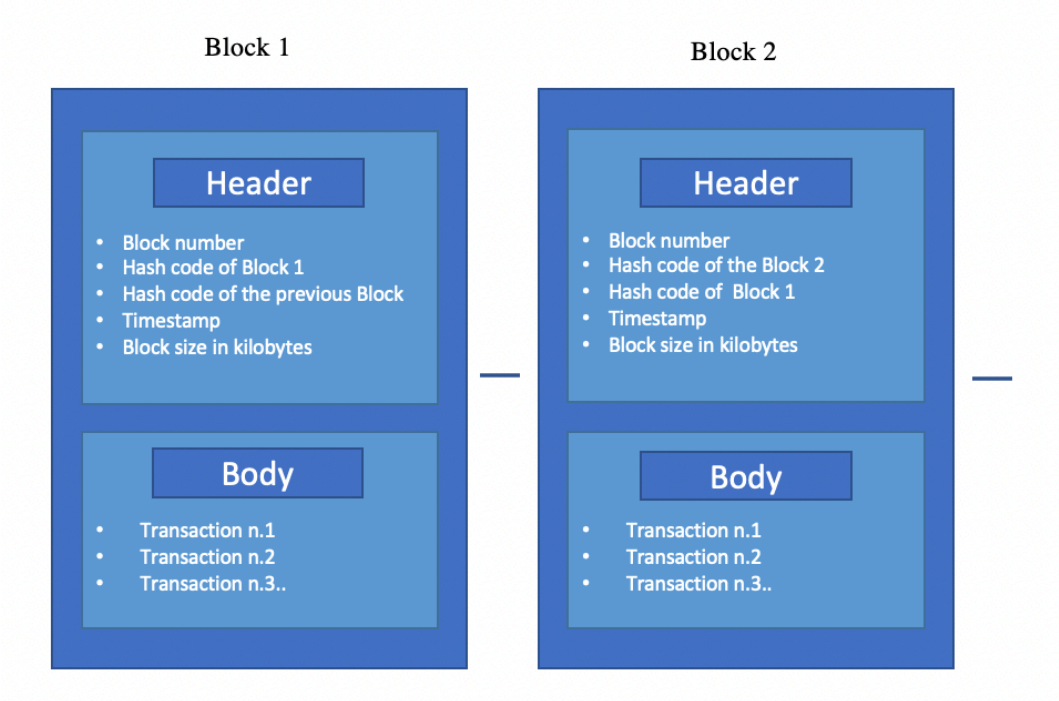
The whole blockchain system exists because the blocks exist, they are composed by two parts: header and body. The header is composed by the number of the block, the hash code of the block, hash code of the previous block, timestamp, the block size in kilobytes.

The body part is composed of all the validated transactions of that block.

The hash code is an alphanumeric code, which has a fixed length and is used to represent words, messages, and data of any length without being able to trace the initial information from it. The second chapter will explain the hash code in more detail applied to the example of Bitcoin Blockchain to make the concept as straightforward as possible directly in its application.

This technology is called a "chain" since each new block contains the ash code identifying the previous block; each block is connected to the previous one and the next just as it happens to create a real chain.

Figure 1.3 Composition of the blocks



Source: our processing

1.1.1 Six Key Technology Features

We can gather the characteristics of a general blockchain in some factors such as decentralisation, traceability, disintermediation, transparency, programmability, and security in transactions.

Starting with decentralization, the information contained in the digital registry is distributed among multiple nodes, thus ensuring security and resilience of the systems even in case of an attack on one of the nodes or in case of loss of a node.

In addition to possessing the inherent security features of a blockchain database, the decentralised blockchain makes use of a peer-to-peer network. Members of this type of network do not need to know or trust each other, and each of them gets a copy of the same blockchain ledger. In this sense, there is no master copy stored in a centralised location and the task of continuously validating the accuracy of the blockchain is left to the significant number of copies generated[8]. Decentralisation also removes the need for a central authority figure and succeeds in keeping out hackers.

Regarding traceability, each element saved in the registry is traceable in every part, and it is possible to reach the exact origin and any changes made over time with absolute precision. The transparency is provided by the ability to be able to watch and control information from across the network. Coletti[9] argues that immutability is a feature of blockchain technology. Thanks to distributed consensus, the entire network can receive approval for data or transactions even when the same environment does not contain trust and is difficult to change. In fact, Derose 2015[10] says that what gives cryptocurrency value is its "resistance to tampering" because

[8] Nguyen C. T. *et al.*: Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks 2019
[9] Coletti, P., 'Bitcoin's baby: blockchain's 'tamper-proof' revolution', 2015
[10] Derose, C., Blockchain for Beginners -Behind the Ingenious Security Feature that Powers the Blockchain, 2015

it has *"the ability to declare a truth, globally and without a center of authority, regardless of what anyone else does to change that truth."*

To what concern disintermediation it can be said that the individual nodes of the blockchain certify the distributed information, thus making the presence of central bodies or companies to certify the data completely unnecessary.

The content of the ledger is visible to all and can be easily accessed and verified by every node in the network but also through services that query the blockchain without making changes. No one can hide or modify data without the entire network learning about it. This concept outlines the transparency[11].
Another characteristic is the programmability in fact, operations can also be scheduled over time, so that certain conditions can be waited for before inserting or modifying.[12]

The last identifier, not of importance, there is the transaction security. In the Blockchain system, the modification of one or more blocks already in the database

[11] Nguyen C.T. *et al.*: Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks 2019
[12] Bonomi Carlo, Assolombarda, Il futuro della blockchain, 2021

is highly unlikely due to the particular characteristics of the verification mechanisms.

If a hacker tried to alter the blockchain, in fact, he would only modify his own copy. This new altered copy would not match the copies stored on the other computers in the network, so the error would be easily discovered.

In the case of a network like Bitcoin, at least 51% of the computers on the network would have to validate the hacker's incorrect version of the blockchain for it to be considered legitimate. Considering the computing power and costs required to affect such a large number of computers in a decentralized network, being able to introduce an error into the blockchain is virtually impossible[13]

1.1.2 Digital signature

A digital signature is a tool for verifying the authenticity of a digital message or document, assuring the recipient that the message was created by the sender who claims it and has not been altered in transit and is therefore intact. At the same time, it provides for the principle of non-repudiation, according to which the sender cannot deny that the message was sent. Blockchain uses a digital signature mechanism based on asymmetric cryptography to verify the authentication of transactions, and its operation is now briefly described. Each user of a blockchain

[13] Nguyen *et al.*: Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks 2019

network has a private key pair and a public key. The private key, which must be kept secret, is used to sign transactions. The signed transaction is then transmitted through the network. The signing phase is followed by the verification phase.

Let's take as an example that Alice wants to send a message to Bob. When Alice finally signs her message, all she does is encrypt her data with her private key and sends Bob the encrypted result along with the original data. In the verification phase, Bob must apply Alice's public key to the encrypted data and checks it with the original data being able to check there has been any kind of tampering[14].

1.1.3 Fork

Inherent to all blockchains are always some kind of exchange unit referred to it, sometimes its cryptocurrencies, sometimes tokens, it depends on the purpose of the project in particular. As time goes on and the functions of each blockchain are used, small or big errors can be noticed, or processes come to light that could be optimized, in short, specific improvements that can be made for that specific blockchain. For this reason, sometimes it is necessary to update the original code and therefore the software of a protocol. If this update is completed the modification is called "fork". Blockchain challenges and opportunities: a survey

[14] Zibin, Shaoan, Hongning, Xiangping, & Huaimin, Blockchain challenges and opportunities: a survey2017

Buterin puts in his paper the focus on the licensing model that allows software changes to a currency platform as well as blockchain applications.[15] Because the blockchain protocol is open-source, changes can be made if a certain threshold of users agree, this practice is commented by Evans, saying that this open-source practice is very important because it allows users to be able to collaboratively modify the platform. [16]

"Open source is a development method enabling software to harness the power of distributed peer review and processual transparency. It comes hand in hand with increased reliability, flexibility and reduced costs"[17].

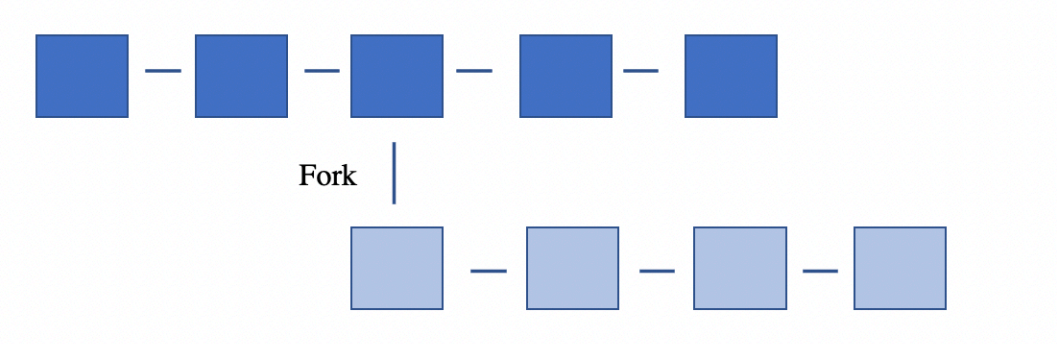
For example, we can take in consideration the Bitcoin protocol. In 2017, there was a fork of Bitcoin, named Bitcoin Cash. Since Bitcoin is the first currency and currently also the most valuable it is not perfect, in fact we can find issues specifically regarding its scalability. The blocks of the Bitcoin blockchain have a limited size equal to 1 MB, with rather long transaction times compared to other new protocols, and therefore the network is not able to handle a lot of transactions simultaneously (from 4 to 7 transactions per second).

For these reasons, after several studies, an update was proposed to increase the block size from 1 MB to 2 MB. The idea was put to vote and 95% of miners were

[15] Buterin (2015a)
[16] Evans David, "Economic aspects of bitcoin and other decentralized public-ledger currency platforms." 2014 page. 4
[17] Open-source initiative, 2015

in favour. This protocol was called SegWit2x, but after being implemented has not shown a resolution to the problem for which it was designed. At this point another update was proposed, that would bring block size from 2MB to 8 MB, this second proposal for a protocol is called BitcoinCash. Given the fundamental change that this implementation has made, it brought a separation from the original Bitcoin network, and this is how a new separate blockchain was formed. Based on the original Bitcoin protocol, but with this big modification, this case is referred to as a 'hard fork'. The Segwit2x implementation on the other hand can be considered as a 'soft fork', since despite the modification there was backward compatibility with the previous blockchain. In other words even outdated blocks are still able to execute transactions and add blocks. In the hard fork the backward compatibility does not exist.

Figure 1.4 Fork



Source: our own processing

In Figure 1.4 we can see what a fork looks like, regardless of whether it is a hard fork or a soft fork since the difference lies only in the protocol rules

1.1.4 Hash function

In computer science, a hash is a function (or a mathematical algorithm) that performs a very specific task: basically, it transforms any string of arbitrary length into a string of predefined length. The output returned by a hash function is called a digest. Words, any text, file or image can be transformed into a hash code. The hashing algorithm is unidirectional. It means that once created, a digest is difficult to reverse. This means that it is impossible to trace back the source text from a hash code. Because of this characteristic, cryptographic hash functions are widely used in computer security areas such as digital signatures, password verification and file or data identification. This mechanism has become so important because the slightest change in the original message results in a complete change in the output hash, even just a comma completely changes the digest. There are many types of hash functions but the one used in Bitcoin is the SHA-256 algorithm. This algorithm returns a 256-bit alphanumeric string. On the web there are many sites that calculate the hash code, we will make an example. Let's try to calculate the hash of the title of this thesis, so we type in "Security Token Offering: Enterprise introduction to Blockchain and funding through STOs." The SHA256 hash that comes up is:

bac02f271483f5b675f30624b00fe797eafd7725c77ffd9be9a6b2e8af7639a7

I now test with the same sentence but adding an endpoint. The SHA256 hash of the new sentence, "Security Token Offering: Enterprise introduction to Blockchain and funding through STOs." is

c3279fa7ed00bf95448b32c133059f0239268e46be83ee4b36df201b004f747f

From this we can see that a small change in the sentence is enough to change the hash code considerably.

1.1.5 Cryptography

As has been well mentioned so far, the blockchain system is protected by cryptography and so is Bitcoin. Data encryption refers to the development of converting data from a readable form into an encoded format that can only be read or processed after it has been described. Encryption is the basis of data protection and is the simplest and most important way to ensure that information on a computer system cannot be stolen and read by someone who wants to use it for malicious purposes. An example of cryptography comes to us from Julius Caesar when, in order to send messages, each letter of the alphabet was replaced with the letter in three successive positions. This is how an 'A' became a 'D' and in order to read it, others would have to know this key. This is how we understand the basis of cryptography, which contains a key, i.e. a rule by which the message is hidden, and a reading key by which it can be read. This method, however, is identified as symmetric encryption because the key is the same for both encryption and

decryption. Nowadays, thanks to the internet and technology, it is possible to talk about asymmetric encryption, which is what is present in Bitcoin and other blockchains. Here, however, the keys for encryption and decryption are different. The invention of asymmetric cryptography is attributed to Whitfield Diffie and Martin Hellman in 1976.[18]

As mentioned, there are two keys: a public and a private key. The public key in Bitcoin also represents the address of the account and this is known publicly, the private key on the other hand must be only and jealously in the possession of the owner of the account because it is with it that they can access and move funds. In summary, Bitcoin's operation revolves around private keys, bitcoin addresses (also seen as public keys and correspondence with the 'account') and digital signatures. The digital signature is made by applying the secret private key and a unique signature is always generated. In cryptography, the term for this digital signature is 'WITNESS'. We find a real mathematical link between the two keys. The private key is used to make digital signatures on messages, this signature is checked for validity by the public key. In this system, however, a problem could arise if an attacker were to intercept the message and modify it using the recipient's public

[18] Whitfield Diffie And Martin E. Hellman, New Directions in Cryptography Invited Paper, 1976

key. This is why Bitcoin uses double encryption combined with a hash function: double hashing SHA-256.

1.1.6. Consensus algorithm

The consensus algorithms are those processes that allow users of the blockchain to coordinate, the ultimate goal in fact, is to be able to ensure that the transaction or information is based on the truth and this truth must be certified in a credible manner, as when a news story comes out on the internet and to have the security of the same are going to seek confirmation in authoritative sources such as the government website or certain portals. This can not happen in blockchain because no node has more importance than another, no information is truer than another unlike the government website for example that has its own credibility.

In this way, consensus allows users and machines to communicate solving the most important problem: trust.

The figure of the validator comes into play with regard to trust: it is the one who must succeed in inspiring trust by proving that he is acting in the right way. The validator, in fact, is the one who wants to contribute to the creation of the blocks. This is possible by making sure that the computer can complete the operations foreseen by the protocol in question and checks the information declaring it true and worthy of certification to close the block. When a node wants to add a block i.e. validate it, it has to put into play amount of value which is called stake. This

happens because it is necessary for this stake to dissuade the variant so that it does not act dishonestly and does not want to be extricated from the system as soon as its dishonesty is discovered by the other components of the network.

In addition to this, there is an incentive to make sure that one does not fall for dishonesty: a kind of reward. Since this node has helped in the formation of blocks and thus to the very functioning of the blockchain it will have a reward as a thank you for being an integral part of the functioning of the whole system. The reward usually consists of a fraction of the native cryptocurrency of the protocol that is formed thanks to the fees that users pay to get their action (information or transaction) certified on blockchain.

1.2 Different types and levels of decentralization

1.2.1 Ledger and DLT

The blocks present and saved in the blockchain are called ledgers. Generally, in history these books were used to keep a proof of trade of goods and services. In the present day they are stored digitally. These properties usually belong to someone and thus possess a centralized trust. The interest being shown lately is in a distributed ownership system. With such an architecture we find a much higher number of computers interested in the purpose than when management is centralized. It is fair to be able to bring to the origin of this interest a matter related

to problems of trust, reliability and security that centralized systems can bring. When it concerns these centralized ledgers then, there are multiple issues that can occur. Some examples are that centralized ledgers could simply be lost due to carelessness, be in a homogeneous network which would mean that every software and hardware component and even the network infrastructure are the same. This as is well understood would result in significant loss of data across the entire system should something happen to the system itself. Even being located in a specific geographical area would lead to problems and make services unavailable in the event of network outages. In addition, there are other issues that can be categorized as trust issues, such as: you can never be sure that the third party you trust is using computer systems that implement best security practices. The user must also trust that the owner's validation actions have occurred well, in order and that they have all been notified and most importantly that they have not been altered.

The blockchain can be considered the best known form of Distributed Ledger Technology.

The DLT then, are a set of protocols, which we can also identify as rules, that allow a network of peer nodes to manage the ledger. As already mentioned, this ledger is owned by all participants who can consult all the evolutions of the updated data. It is also protected by encryption. From this it follows that no central body controls the entire system. Specifically those protocols that control the updating of data through structures that are concatenated together and protected by cryptography.

What differentiates DLT from Blockchain is the fact that precisely each node has a full copy of the ledger. Summarizing: all blockchains can be DLTs but not all DLTs are blockchains.

In DLTs, unlike centralized ledgers, the control of data actions is shared only by some network actors, in blockchains this information is available and the ledger is shared with all network participants. It is always good to remember that however Blockchains remain a sub-set of DLTs. There is a move towards DLTs not only as a decentralized system but as a distributed data record. New possibilities customized to the needs of businesses are being glimpsed. DLTs have dynamics to determine who can enter and how much "share" it takes to make a decision. In conclusion, blockchain types are identified with respect to who makes the decisions (Permissioned or Permissionless Blockchain). [19]

[19] Word Bank Group , Distributed Ledger Technology (DLT) and Blockchain, 2017

Figure 1.5 DLT Application potential

Overview of Potential DLT Applications (at varying stages of development)	
Financial Sector Applications	
Money & Payments	• Digital currencies • Payment authorization, clearance & settlement • International remittances and cross-border payments (alternative to correspondent banking) • Foreign exchange • Micropayments
Financial Services & Infrastructure (beyond payments)	• Capital markets: digital issuance, trading & settlements of securities • Commodities trading • Notarization services (e.g. for mortgages) • Collateral registries • Movable asset registries • Syndicated loans • Crowdfunding (as initial coin offerings) • Insurance (in combination with smart contracts) for automating insurance payouts and validation of occurrence of insured event
Collateral registries and ownership registers	• Land registries, property titles & other collateral registries
Internal systems of financial service providers	• Replacing internal ledgers maintained by large, multinational financial service providers that record information across different departments, subsidiaries, or geographies

Source: Distributed Ledger Technology (DLT) and Blockchain, Word bank Group.

1.2.2 Permissionless and permissioned Blockchain

The idea is that there are multiple types of blockchains and they differ depending on the number of actors that can make decisions within the network and therefore also different types of consensus. In this case, blockchains can be: permissionless or permissioned. [20]

Two examples of the permissionless blockchain type are Bitcoin and Ethereum. We can specify that in this category there is no need for an authorization from someone

[20] Bonomi Carlo, Assolombarda, Il futuro della blockchain, 2021

to perform an action. They do not have property rights or a central authority of reference, therefore, they can not be controlled, and anyone can access them. Since there is no one who can block the path of the transaction, that goes up to the insertion in the block, which prevents any form of censorship. For those reasons the permissionless blockchain can be used as a global database for documents that by their nature need to be certain, so they can not not be tampered with[21] grants all users or nodes read access and the right to write and verify new transactions.[22]

Private blockchains on the other hand are called permissioned, they lack the feature that represents some of the most important advantages of the technology: decentralization. They are managed by one or more organizations and have a central entity and is based on a set of rules. The components are therefore selected from the beginning, and this gives them a very precise composition. Permissioned blockchains are divided between public permissioned and private permissioned. In the private permissioned those who have an interest in going to read or access the creation and completion of a transaction must have an authorization, so nothing that is not authorized will be allowed. When instead we talk about public permissioned, we mean that users, who are part of it, since we are not talking about a permissionless blockchain, can access information and implement operations.

[21] Comandini Gianluca, Da zero alla luna, pag 67
[22] Garzik Jeff, BitFury Group, Public versus Private Blockchains, 2015, pag. 11. https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf

These types of systems are mainly used by large companies or institutions for a more optimized management of time, resources, information, greater organization, and reliability. In this case they are defined as 'blockchain belonging to a consortium'. In this regard we have as an example the R3 consortium which consists of technological research and is formed by large companies including Bank of America, Royal Bank Canada, National Bank of Australia, etc.

Chapter 2. Cryptocurrencies as the Blockchain frontier of finance

2.1 Consensus algorithm application

2.1.1 Proof of work

In 1977 a UK cryptographer and businessman, Adam Back, proposed the 'hashcash' protocol to try to put an end to the problem of spam in e-mails.

Hashcash was the first proof-of-work algorithm; it required work to be done by the client. To send the mail, two more fields had to be added, additionally to the regularly required, the nonce and the hash.

Back argued that by making the process of sending 'spam' e-mails more laborious, they would be reduced. According to this protocol, in fact, a code had to be added to the header of the mail, this operation confirmed that the sender had spent time and computational capacity to send the email. This code had to meet certain

parameters to be valid and this required time and resources. This meant that sending e-mails to more people was made more resource intensive.[23]

Later on, Nakamoto in 2008 with the publication of the withe paper of Bitcoin took the existing concept and opened it up to a wider audience.

Nathaniel Popper in his book "Digital Gold" described Proof of Work (PoW) in reference to the Bitcoin system as follows: "It is relatively easy to multiply 2,903 and 3,571 using a piece of paper and pencil, but much, much harder to figure out what two numbers can be multiplied together to get 10,366,613."

This is exactly the kind of work that a computer must complete when using the PoW system.[24] Proof of work is a consensus algorithm that enforces the creation of new blocks on the blockchain, Bitcoin uses this type of system and currently Ethereum but not for much longer as there will soon be a change of consensus algorithm from proof of work to proof of stake. The use of proof of work can be explained as a mechanism to ensure that transactions between two users are unlocked and therefore executed. Since the validation of transactions gives a reward in return, there is a competition between those who wish to finish the work and take home 'the gift'. Those who carry out this action are identified as Miners precisely because the name shows parallels to the work in traditional mines. The computer works to

[23] Rubino Alessandro, Network Digital 360, Proof of work: cos'è e le differenze con il proof of stake April, 2022https://www.blockchain4innovation.it/criptovalute/blockchain-cosa-sono-i-protocolli-pow-e-pos-e-a-cosa-servono/

[24] Conway Luke, Blockworks,: Proof-of-Work vs. Proof-of-Stake: Which Is Better? February, 2022

solve a mathematical problem that manages to unlock the transaction. This reward is a coin that has been created by mining. When the block is created, a fraction of the value of the cryptocurrency of the blockchain on which it is operating, is created and this is the share that the miner receives for its computational power.

PoW is based on cryptography, hence the name 'cryptocurrency'. Cryptography is used to decide through what type of consensus is reached in the blockchain and thus the validity of transactions. Cryptography is developed with mathematical equations that not all computers can solve, but only those with high computational power. None of the problems that have to be solved for consensus are the same as others to prove that the transaction is Authentic.[25]

These mathematical problems are different and may include calculating an input hash function from an output hash function, decomposing a number with two primes or a guided tour puzzle protocol or identifying a chain from an alphanumeric code. Users want to mine that means to contribute to the network and receive the rewards. The more the network expands, the problems to be solved become more and more complicated and this is where some problems can arise. Having a functional plan for the complexity of the problems to be solved is essential, they have to be balanced and this is a job done by the algorithm itself. You can identify the added value of a blockchain, among other things, with the speed of the process

[25] Tar Andrew, Cointelegraph Proof-of-Work, February 2018
https://it.cointelegraph.com/explained/proof-of-work-explained

but if the problems are thought to be highly complex, the computer will take a long time to solve it and this could create a clog in the network and make it slow. In addition, the same problems that are solved must be able to be easily verified by other nodes, because transparency is the primary principle. For these reasons, the question of the difficulty of the problems is very relevant. The proof of work algorithm is implemented with the miner that solves the mathematical problem in order to certify a block and close it. This means that also the information inside it is confirmed. The block that will be created will have an hash and will also contain the hash of the previous block to create a chain.

"The blockchain is a chain of transactional records that a subset of network participants (also known as 'miners') enriche by solving difficult computational problems. Miners fiercely (and anonymously) compete on the network to solve the mathematical problems in the most efficient way, thereby adding the next block to the blockchain. The block reward (i.e. newly mined coins) is sent to the miner's public address. If the miner wants to spend these coins, (s)he must sign with the corresponding private key. When system-wide mining power increases, so does the difficulty of the computational problems, required to mine a new block (Böhme et al, 2015, p. 218). This difficulty level is adjusted to keep the block-generation pace constant, roughly ten minutes (Dwyer, 2014, p. 5). "[26]

[26] Pilkington1, Blockchain Technology: Principles and Applications, 2016

The only way to act dishonestly in proof of work would be to control 50% plus 1 of servers and then be able to get this percentage of servers to say that the transaction taking place is real. This could mean for example that if Matteo sends some money to Andrea and Matteo could control the 50% plus 1 unit of the computational power , by confirming that this sum has actually been sent, even if he has no intention of sending the money, the transaction will be validated. It would therefore seem that this blockchain is not secure, but in reality, it would be impossible to get these percentages to succeed in forging consent. In any case the costs of controlling the 50% plus one server would be far greater than any amount that could be transferred.

The miners are the first to be interested in how the protocol works because they hope to get something out of the validations. They also believe strongly in the project that makes them act in order to let the system continue to work. To summarize, the willingness to get money is based on the working of the blockchain system, if it should stop working, nodes would lose all the value. These two aspects highlight how valuable the technology is to the community that is discovering it.

"*Notwithstanding the existence of personal motives, there might exist a cooperative behavioral dimension in sharp contrast with a neoclassical economic arena dominated by Darwinian principles*. *The high level of energy consumption of PoWs as shown by de Vries (2018), explains the energy costs that this protocol requires.*

In fact it is considered as one of the biggest reasons that are accelertion the shift from Proof of work to proof of stake as Irresberger et al. (2020) argues.[27]

2.1.2 Proof of stake

This consensus algorithm, like all others, is also tasked with ensuring the integrity and security of the information stored on the logs through adherence to the rules of the protocol. Proof of stake is alternative to proof of work that was proposed after taking into consideration that PoW actually required a lot of electricity to work. King and Nadal (2012)[28], were the ones who first proposed pulling the PoW directly from the Peercoin blockchain project. As by Irresberger et al. (2020) [29]lately the amount of blockchain with proof of stake system has grown, in fact he reports in his paper that since 2015 at least 50 projects have been developed with this consensus algorithm.

The Proof of stake algorithm gives very precise indications on how to proceed with the addition of blocks, the time is in fact divided into periods (time slots), the algorithm makes sure that only one block at a time can be added to the blockchain. This allows not one branch of the chain to grow more than the others in a given time slot.

[27] Pilkington1M., Blockchain Technology: Principles and Applications, 2016
[28] King Sunny and Nadal, Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012
[29] Irresberger Felix et al. The Public Blockchain Ecosystem: An Empirical Analysis, 2020

During this time slot, the algorithm randomly searches for a coin and when it finds it, it can also recognize who is the owner of that single coin it has 'extracted'. The owner of this coin thus has the possibility to add a block to the chain. From this we can derive that the one who possesses more coins, is the one who has a higher percentage of probability to be elected rather than another with a smaller number of coins in possession. [30]

The validator in this case is no longer chosen based on its resolution of the mathematical problem but rather due to the amount of stakes they possess.

The only incentive for miners in this system are the transaction fees associated with the specific block created. The method entrusts consent to network users who hold a certain, arbitrarily defined amount of a certain cryptocurrency. This amount will be effectively 'frozen' as collateral. In case of misbehavior or malicious attempts to validate incorrect transaction blocks (transactions that withdraw coins from the wrong user, or deliver it to the wrong user), the malicious validator is punished. Depending on the severity of the act, he/she may lose part or all of his/her frozen amount. So, to be chosen as a validator you have to own and stack a quantity of cryptocurrency from that blockchain, and this quantity of the stack indicates the probability of being chosen as a validator of the next blockchain.

[30] Fahad Saleh, Blockchain Without Waste: Proof-of-Stake, pag. 10

As argued by Cong T. Nguyen on his paper, “the probability *pi* that node *i* is selected to be the leader in a network of *N* participants is [31]

$$p_i = \frac{s_i}{\sum_{j=1}^{N} s_j},$$

where *si* is the stake of participant *i*. This means that the more stake a node holds, the higher chance it is selected to be the leader. “

In the case of proof of stake, validators are rewarded not with the creation of an amount of cryptocurrency allocated to them (as in POW), but rather with fees paid by the users who carry out the transactions (just like bank transfer fees). [32]

2.1.3 Comparison

The debate on proof-of-work and proof-of-stake might seem technical at first glance, but it is not. In fact, it reflects the differences in approach of two mechanisms that have the same objective. The substantial differences involve network security, eco-sustainability, barriers to entry and decentralization.

The objective of a blockchain system is to ensure that transactions are processed and recorded as intended, i.e. peer to peer (no mutual trust or intermediaries are needed). Regarding the two major consensus mechanisms, we can identify what

[31] Nguyen Cong T., Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities , 2019

[32] Nguyen Cong T., Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities 2019

their strengths and weaknesses are. The first weakness of PoW is certainly energy consumption, since solving mathematical problems requires electricity and the computational power required consumes a lot of it. In this type of consensus, since 'work' is required, the time needed to carry it out can compromise speed. The weaknesses of the PoS are of a different nature, for example, the amount of money you have in staking is locked so you can't move it or sell it for another type of currency, and in general the richest nodes are more likely to be chosen to validate the block. Since it is still a new methodology it is a little less secure about haking attack compared to PoW. Dealing with the positive aspects at this point it can be confirmed that PoS requires less computational power and is therefore more energy efficient, it does not require specialised equipment and the entry barrier is less high than that of PoW. PoS manages to guarantee a higher transaction speed. Among the advantages of proof-of-work is a high level of security, which makes external attacks difficult. It also manages to maintain a higher level of decentralisation because it depends on the work that is done and not on how rich you are in staking. The Ethereum blockchain is currently in the process of migrating from the proof-of-work blockchain to the proof-of-stake blockchain with the 'Casper' operation. Once operational, proof-of-stake will be more environmentally sustainable, as it eliminates the large amount of energy required to create new cryptocurrency. According to Vitalik Buterin (the founder), the change will reduce Ethereum's energy consumption significantly.

In recent years, various consensus types are also being experimented with, the idea being to arrive at a version that is better than all of them in several respects. However, apart from POW and POS the others such as Proof of Identity, Proof of Authority and Proof of Concepts are used to a lesser extent. To overcome the problems of the main consensus algorithms, hybrid forms of the two main ones have also been implemented, such as proof of activity[33]

This for example creates empty blocks with the POW while the POS algorithm is used to verify and enter transactions. The Snow White protocol is based on PoA[34] and in this case PoS is employed to select candidates while then PoW is used for a competition between the candidates and the winner creates the blocks. In any case, these hybrid protocols contain both the positive and negative sides of the mechanisms from which they derive. In fact, in each case for example the energy consumption will be less than that of pure PoW but higher than that generated by PoS.[35] In the blueprint for a new economy, Swan[36] reasons whether information brought by a consensus (consensus as a general concept) is a different type or form of information, according to his thinking there are at this point three types of information. The first concerns raw information, not simply improved information

[33] Bentov I., C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake" ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34-37, 2014.
[34] Daian P., R. Pass, and E. Shi, "Snow white: Provably secure proofs of stake," Int. Assoc. Cryptolog. Res., Tech. Rep. 2016/919, Sep. 2016.
[35]Nguyen Cong T., Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities, 2019.
[36] Swan Melanie, Blockchain: Blueprint for a NewEconomy, 2015. Pag 95

as it is. The second is identified with this information plus the context with data that is enriched by social recommendations whose dissemination has been enabled by the internet. The third and final level is through the blockchain, which is an even higher level of recommendation since it has been validated.

The third, and therefore last, is the one through blockchain which is an even higher level of recommendation since it has been validated. This third level is based on the accuracy and quality of the data confirmed by peers, but also and above all by an intelligent structure. This information, in fact, is shaped with intelligent tools that filter its quality, and truth and guarantee its freedom.

The quality of data, therefore, is given by the confirmation of a crowd and here arises a question for consideration: How will the society act with this kind of widespread process for data quality?

One can think that the blockchain could then be "*precisely the kind of core infrastructural element as well as scalable information authentication and validation mechanism necessary to scale human progress and to expand into a global society. The speculative endgame vision is that the universe is information, where the vector of progress means transitioning toward higher-resolution information flows. Information may be conserved, but its density is not. "*[37]

[37] Swan Melanie, Blockchain: Blueprint for a NewEconomy, 2015. Pag 95

Melanie Swan is not the only one asking questions about the future coexistence with these super-technological and avant-garde systems, and Marc Pilkington, in his pepar, as we shall see later on, talks about smart contracts and codes and brings to light a reflection on this coexistence.

2.2 Bitcoin

2.2.1 What is Bitcoin

To talk about Bitcoin (BTC) we must first distinguish between the Bitcoin blockchain and the bitcoin cryptocurrency. The capital letter or small latter of the "B" can differentiate the context we are referring to. In fact when it is starting with the small "b" it is referred to cryptocurrency and when it is the capital "B" it refers to the blockchain protocol where bitcoin runs. This confusion can only occur with Bitcoin as other currencies usually differentiate the reference to the network rather than the cryptocurrency or token being referred to. For example in the Ethereum (ETH) blockchain the cryptocurrency is referred to as Ether. Bitcoin is an open source protocol released in 2008 by its developer Satoshi Nakamoto.

The smallest unit into which to divide bitcoin is called Sathosi, it allows for great payment flexibility. The Euro for example is divisible into 100 cents, bitcoins are divisible into 100,000,000 Sathosi. This allows for balances up to 8 decimal digits. Satoshi's goal was to create a peer-to-peer system for the transfer of value without the need for financial institutions. Prior to Bitcoin there were other attempts at

digital currencies. In the 1980s, David Chaum had already tried to propose some sort of mechanism to put an electronic signature on the currencies. In the late 1990s, however, there were several research movements that had spawned some projects such as: Hashcash, B-Money, Bit-Gold and RPOW. Undoubtedly, these projects opened up a little bit to the application of digitization, algorithms and cryptography. The only difference with Bitcoin is that these projects had a centralized organization, but Bitcoin remains one of the best implementations of the cryptocurrency concept. Satoshi designates the protocol as a cryptographic and pseudonymous structure that can protect users' identities and facilitate the exchange of value *Bitcoin is thus a collection of concepts and technologies that form the basis for a digital money ecosystem among participants in the bitcoin network.*[38] Since it is a decentralised system and each part contributes to its operation, it is more likely to be able to protect itself against external attacks or errors. In any case, each action involves only the two parties involved in the transaction who reach a consensus via the network.

When we make a payment by credit card for example, the intermediation of a clearing house is required and transactions are commonly handled in mainframes where the concept of scarcity does not exist. In fact, in classical computing anything can be duplicated, Bitcoin in this respect ensures that each individual coin is only

[38] Antonopoulos Andreas, Mastering Bitcoin, 2017

spent once, counteracting the phenomenon of double spending. The electronic currency in question has the characteristics of being an accounting unit,
it allows the transfer of value between parties and is a way to store value that every currency possesses.[39]

As has been explained in the previous paragraphs about blockchain in general, Bitcoin works in the same way. In decentralised management, each node owns an up-to-date copy of the ledger, in each case there is a history of the information. Bitcoin nodes are called miners, precisely because of the work they do (PoW) which ends with the confirmation of the block and the creation of a percentage of the currency. It is in fact thanks to this process that by the year 2140 there will be around 21 million bitcoins in circulation. The protocol has a series of algorithms within it that make it possible for someone to validate a block every 10 minutes or so. It also halves the speed at which new bitcoins are created when a new block is closed. This happens every 210,000 blocks (approximately 4 years). It is thanks to this mechanism that in the long run the bitcoin currency is deflationary.

It is possible to identify this blockchain as permissionless anyone can be a node and connect to the network without any need for approval or identification. As already mentioned every miner who wins the PoW race and thus can create a block receives a reward. Another component of the Bitcoin architecture is the Wallet

[39] Attico Nicola, blockchain guida all´ecosistema, 2018

where users can manage their funds. Bitcoins are in fact associated with an address (which can be imagined as a bank account number). These addresses are protected by two keys, a public key and a private key. These keys are cryptographic and have the function of identifying the users with whom they are associated and making transactions between users actually feasible. They are used to block funds and allow exchanges to take place. They therefore provide irrefutable proof of ownership of bitcoins. We understand how cryptography plays a very important role in the blockchain system.[40]

To conclude we can identify four innovations in cryptography and distributed systems assembled into one. Being a peer-to-peer (decentralised) protocol, consisting of a public ledger, having a set of rules for transaction validation and currency input and being able to obtain a shared consensus through Proof of Work.

2.2.2 Wallet, Private and Public Key

Wallets are bitcoin applications with their own interface that allow the storage of the address and public key. There are many implementations of bitcoin wallets and each user can choose the one that suits them most. So there are wallets which are possible to access via desktop, or only via browser or as phone applications. Also much simpler is the paper wallet which means you can store your keys and personal addresses offline. These are usually called 'cold wallets'.

[40] Attico Nicola, blockchain guida all´ecosistema, 2018

With respect to these two keys one thing that concerns the Bitcoin blockchain most is how to store them. As has been mentioned, the loss of keys equals the ultimate loss of funds, there have been plenty of cases where bitcoins were bought when its value was still very low but without much care the keys were lost to access and prove ownership. There is no appeal to anyone in this case, there is no password recovery as you can trivially do with social or email. There is an alternative to this, which is to buy and hold your own funds in an Exchange without having an external Wallet. In this case the funds are associated with you through a KYC (know your customer) process. KYC is a process where you are identified by official documents (ID or Passport) and you only have one password that identifies your account and in case of problems you can get it back. The downside of exchanges is trust, since if something happens to the platform or has malicious intentions, you lose all your funds. The private key is in fact a binary or hexadecimal string, and is called a Master Seed (when the words are hashed, that type of identifier is obtained and is reversible).

For the sake of convenience of the Seed's storage, a mnemonic code has been implemented that converts the code into a series of words that can be more easily stored and decreasing the possibility of error when transcribing the key. As introduced, the cryptographic algorithm on which the production and interaction of Bitcoin's keys is based is called Elliptic Curve Digital Signature Algoorithm (ECDSA). From this protocol comes the private key which is a random number

between 1 and 1.158x10^77 and the public key which is derived from the private key. Since the ECDSA protocol is irreversible, the public key can be obtained from the private key, but the reverse procedure is not possible in any way (the mathematical function used is unidirectional).

2.2.3 Address and transactions

In the Bitcoin protocol public, private and address keys are all three different. As has been widely discussed the public key is derived from the private key using ECDSA algorithm, the private key is composed of mathematically generated random character strings. From the key pair then only one Bitcoin address can be derived. The Bitcoin address is derived from the transformation of the public key using one of the hash functions, in this case RIPEMD 160. From this step the encoding is done with the BASE58 function. The result is a Bitcoin address, which is an alphanumeric code consisting of 34 characters with the number 3 or 1 as the initial numbers of the string. Transactions at this point take place in pseudonymity and not anonymity because it is true that no identification document is required to have a Bitcoin address but everyone is identifiable through cryptography. In fact, it is only through the possession of my private keys that I can claim to be the owner of those bitcoins inside, keeping in mind that every blockchain action is transparent and traceable. Satoshi Nakamoto's goal was the absence of necessity of a third party to authorise it by taking a commission for the service. Therefore there is the need

for a public network of users who can view and control the order of transactions to ensure that the user who is sending that money is actually in possession of it. This is done by checking each transaction and going back through the chronological order to the actual balance of the wallet. At this point we need the address to send the bitcoins to, which identifies the wallet. The wallet will contain the private key which allows you to sign the transaction and prove their provenance. Now the sender signs the hash of the transaction and adds the public key of the receiver. This is the moment when the network of nodes comes into play: they are in charge of checking and validating the cryptographic signatures and proving that the transaction is permitted.[41]

2.3 Ethereum

2.3.1 What is Ethereum

Until now it has been primarily discussed how Bitcoin was for online financial functions. A bit like online banking for transactions. Ethereum on the other hand aims to replace third parties on the internet, i.e. those that currently hold our data (Google, Facebook, Amazon etc). The Ethereum white paper was presented in 2013 by Vitalik Buterin, this document describes the functionalities, purposes and processes that characterize the technology by its creator. A white paper exists for each blockchain and can always be consulted. In the case of Ethereum a Yellow

[41] Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System

Paper was also published in 2014 to add further specifications. Butering and other guys who make up the team that developed the blockchain set themselves the challenge of going beyond a 'computer currency' and creating a system in which computers have to abide by well-defined rules. These rules are defined in contracts, smart contracts. These smart contracts are detailed, very articulated and allow all the conditions to be mathematically executed by the algorithm, that are needed to be able to protect the personal data or preferences of users. The idea is to have a super computer that is always connected because it is composed of the network of computers that are part of the blockchain. This EVM, Ethereum Virtual Machine, is a real computer made up of many where programs are run in compliance with laws. Programs or applications that can run on Ethereum are programs that were previously used, ran on a centralised computer or server, and were programmed with a standard programming language. The reason why Ethereum is so powerful is because it gives you the possibility to use applications without having to create your own blockchain. These applications are programs written in a programming language that programmers already know about. In addition, the Ethereum network is always active thanks to its servers, and since they run in a decentralised network, they are less likely to be hacked or shut down (go offline), and the computing power is far greater than that of a single computer. Companies for example can design their own applications and use Ethereum as a platform to get them up and running instead of having to structure and design a new blockchain. In Ethereum it is

therefore possible to carry out transactions as well as develop applications (dApps) and run smart contracts. Ethereum has its own cryptocurrency Ether (ETH), it is generally identified as 'Fuel' for the network itself and therefore called Gas. When transactions are made, these have a commission cost and in jargon they are called Gas. The Ether therefore remains a cryptocurrency and means of payment but unlike the others can also be used to speed up the processing of DAPP. In fact, the more Gas you are willing to pay, the sooner the operation will be carried out. The fee to be paid for transactions/operations also depends on how much processing is required for that action. An important aspect is that unlike bitcoin, the total amount of Ether is not fixed. It is continuously created depending on demand. As with Bitcoin those who participate in the Ethereum network are part of a Peer to Peer network, Ether is a decentralised cryptocurrency using cryptography. The unit of measurement of Gas is called wei. Ethereum is also based on proof of work, although its team has announced a transition to proof of stake soon. [42]

2.3.2 DAO and DAPP

The origin of the DAO comes from Werner Dilger, a German computer scientist who in 1997 worked on the 'decentralised autonomous organisation of the smart home according to the immune system principle'. At that time, this innovation could not be practised. With the advent of the blockchain the possibility of being able to

[42] Buterin Vitalik, Ethereum white paper, 2014

implement it was unlocked, this happened with the creation of Ethereum by Buterin in 2015.

One of the most important and significant events that have marked the history of Ethereum is the DAO. DAO stands for Decentralized Autonomous Organization, it is literally an organization built on Ethereum and based on smart contracts. It acts as a program that runs on the blockchain with a financial base and issues shares (tokens). These shares are acquired by paying in Ether. The main objective of DAOs is to create a company that functions properly and completely without any hierarchical management. It therefore operates as a real company, but the management is automated and decisions are made by those who have bought the token of the DAO of reference. With the capacity of DAOs being able to programme and carry out certain actions according to certain rules, they are autonomous. The way to program these rules is to use the smart contract that enforces the rule 'code is law', referring to the code and everything that is programmed, the conditions inside act as the law.

A DAO can be understood in a condominium context. For ecxample the maintenance funds can be deposited through the actions of smart contracts. Now the funds are not in the hands of anyone but are decentralised, every tenant knows the rules (because they are engraved in the smart contract). When an offer of the maintenance arrives and is chosen by consensus, the DAO would release the money by having the majority of votes, as it is stated by the inherent code that that

particular maintenance is necessary. The DAO should not be confused with DAO in general. The DAO was a case that exposed some downsides of this technology. In 2016, a hacker managed to seize $50 million in Ether through a vulnerability of the smart contract code. The story shows how important the proper programming of smart contracts is, a misplaced smart contract does not mean the failure of the project because if a website doesn't work, it doesn't mean that the internet is 'broken'. Dapps are nothing more than decentralised applications, and are another feature of ethereum. Users connect to each other exactly as explained in the concept of decentralisation. Even if a company or a developer devises a dApp, once it has been put on the ethereum blockchain it is no longer controllable by the person who made it. Control will be given to the majority of users. To explain the concept well, the reference can be to Gmail. When a user sends an email, it goes to the gmail server which then passes it on to the recipient. All mails are kept by the server, it is the server that carries out the transfers. If, for example, the server fails, no e-mails will be sent, and if the server is hacked, someone can get hold of private e-mails. Such an episode could not happen in the case of dApps because the computer network makes availability permanent via the network, and thanks to the blockchain properties, hacking is improbable.

2.3.3 Smart contract

Smart contracts are one of the main innovations of Ethereum, they could have even more surprising consequences in the world of finance and contracts. Smart contracts are exactly like legal contracts with the difference that instead of being composed by lawyers, they are written by programmers and do not contain words but code, and are able to self-enforce.

They are written in source code using the solidity language and run on Ethereum's virtual machine and blockchain. They share the use of the Ether currency, through which every payment is made. The standard contract always contains conditions in if clauses: "if it is this, then that". This means that the conditions are fixed by the code. It is possible to refer to the example of selling property. The smart contract is programmed in such a way that at the exact moment when money is exchanged, the property is replaced simultaneously. However, if by chance the debtor pays less money than agreed, the smart contract will not see its pre-programmed conditions as fulfilled and will not exchange the property. In general, they can contain fees and compensation if a part of the contract is not fulfilled. One of the positive aspects of smart contracts is the absence of misunderstandings that can occur in traditionally enforced contracts. A comma or a grammatical error can completely change the meaning of a sentence. Lawyers and courts are not needed to enforce them. As soon as the contract is fulfilled by all parties, it will be executed. If, however, for some reason not all terms are met, the contract will be terminated automatically and

compensation will be executed directly. Executing contracts on a decentralised blockchain reduces the risk of hacker attacks. The changes you make to the contract are recorded on the blockchain, thus making them transparent. Although the advantages are manifold, so are the disadvantages. First of all, there are currently few real-world legal requirements, meaning that there are no real guidelines yet. Furthermore, it is still difficult to program a contract for the quality of a certain thing, since only if clauses can be met, for example, it can be said that an action has been carried out but it remains impossible to quantify the quality of execution. [43]

2.3.4 Token and Gas fee

When executing transactions in Ethereum, each action is executed and accounted for according to cost, which in this case is called Gas.

Gas has a counter value in Ether which depends on the market performance. A distinction has been made to differentiate the computational expenditure in terms of energy from the purely economic one, whose value depends on the market. Therefore, when transactions are executed, i.e. there is a 'call' to execute a certain contract, there are two terms: Gas limit and Gas price.

The gas limit is your choice of how much you want to pay for a transaction. In fact, you can decide how much to pay (within certain ranges) and consequently you are

[43] Makoto Yano, Blockchain and Crypt Currency, 2020, chapter 5 https://ethereum-news.it/ethereum-gas-cost-fees/

told how long your transaction will take to be approved. The more you pay, the shorter the waiting and validation time will be, and this can be adjusted during the processing of the action if it does not go through as intended. If I set the gas limit too low, no validator will be motivated to execute my transaction and so it will not be taken into account. The gas price is what you actually pay at the closing of a transaction. It is usually an average value to the reference value and also gives an insight into how to set the Gas limit. Unlike cryptocurrencies tokens do not have their own blockchains.

Tokens are digital assets created within existing blockchains. They can only be transferred between wallets on the same blockchain. In order to carry out any transaction, Gas fees must be paid with the blockchain's native cryptocurrency. For this reason, the wallet holding the token must also hold a small amount of the native cryptocurrency of the relevant blockchain. It is important to remember that if a token is sent to a wallet on a different blockchain network than the one on which it was created, the funds will be lost.[44] [45]

Tokens are a representation of a value that will be useful depending on the reality in which it is placed; in fact, there are various types of tokens that have different functionalities and a countervalue in cryptocurrencies. This representation of value

[44] Nova Sera, quali sono le differenze tra criptovalute e token? (2022)
[45] Oliveira, Luis; Zavolokina, Liudmila; Bauer, Ingrid; Schwabe, Gerhard. University of Zurich: To Token or not to Token: Tools for Understanding Blockchain Tokens, 2018

can be used within the blockchain in which they were created. A token, therefore, specifically, is a digital asset based on the blockchain that can be exchanged between two parties without the need for the action of an intermediary. Tokenisation (i.e. the process of linking value from the thing/information/rights that will be represented by a token) has been used for example in real estate where property has been divided into many small shares to be sold to investors in a process of "democratizing" shareholding. Furthermore, it has many other applications, such as the tokenization of works of art, in the world of sports and, above all, the use of the informatics tokens can be very important at the financial level in the Stock Exchange sector. Obviously, to do this there needs to be a process of converting company shares into tokens. The tokens represent real assets.

The reality of tokens is very wide, apart from the ones already mentioned above, even a blog article, a book or a song can become a token and it ranges over many sectors. In the next chapter we will discuss tokenomics[46] related to capital racing, where tokenisation in the financial sector is the central part of the implementation.[47]

[46] Tokenomics, a term that represents the economy and tokens therefore the token-based economic ecosystem.

[47] In this section the token is explained in a general way because it is part of the Ethereum reality and has been named for completeness. In the next chapter there will be in-depth analysis of different types of tokens and their functionalities on the Ethereum network with the final aim to refer mainly to the capital raising modalities.

Chapter 3. Blockchain Application Domains

3.1 Blockchain use-cases in Real-World industries

The inherent characteristics of blockchain technology mean that it can be applied in many areas. Below are some examples and in the next chapter we will also go into the application of the technology to finance.

In the supply chain, logistics providers are heavily relied upon to deliver the goods needed to manufacture finished products and to get these to their customers. Using blockchain, transactions can be independently verified, recorded and co-ordinated without the intervention of third parties, making them simpler and without intermediate impediments. By implementing a unified digital document management strategy, all supply chain participants can track the location of cargo and products. In addition, this technology provides data that, in most cases, can eliminate any payment disputes. Regarding the payment of suppliers in the electronics industry for example, blockchain technology allows suppliers to be paid directly on the strength of encrypted distributed ledgers that verify transactions in real time. This mechanism eliminates the need for intermediaries such as banks and automatic counterparties (clearing houses), thus improving efficiency.

"There are a number of potential use cases: managing electronic medical record data, protecting healthcare data, safeguarding genomics information and tracking

disease and outbreaks, to name some," said David Brown, science and program director at Qatar Precision Medicine Institute. The development of technology related to healthcare has great potential.

Just consider the multitude of documents that each person must have and the quality of information that reaches doctors. If an elderly person forgets an important document to bring to the doctor's supervision, the care assigned to him or her may not be suitable. Having a record of complete information about the state of health, on the other hand, would have a more practical and quicker approach.

Blockchain technology could also help in charity because of its fundamentals. Transparency and traceability are the basis for a reliable and worthy charity campaign. It could also bring a resolution regarding resource management. A significant example is the Blockchain Charity Foundation.

Within the public administration there are some interesting examples for a hypothetical development of the technology. It would bring benefits with regard to digital identity, the archiving of court decisions, the financing of school buildings and the tracking of money, civil status, electronic voting, business licences, criminal records and even tax documents. All this thanks to, among other things, the potential for data management and the traceability of transactions without the possibility of information destruction. For example For voting, blockchain eliminates the scope

for voter fraud as the data is immutable so no one can change the file in the ledger. It also provides the option to vote online via a secure platform. In this way, each vote goes through a verification process to confirm its identity.

For the energy sector, blockchain can bring a significant improvement in resource efficiency. In this regard, there is an EU-funded project, PlatOne, which aims to realise the management of electricity transmission and distribution networks.

The real estate sector can also benefit from the use of blockchain-based smart contracts. An experiment in the field of real estate auctions is being carried out by the T6 observatory and the Italian Blockchain Association. The two organisations are engaged in a kind of digital cataloguing of all real estate assets at auction. In practice, in a blockchain, the data relating to the real estate subject to execution is recorded, so as to have a history of the legal, financial and urbanistic vicissitudes of each property. The aim is to make the tool usable by public entities, such as the courts, or even private individuals, so as to exploit digital technology to streamline and speed up all the processes and administrative steps linked to auctions.

Regarding art and entertainment, technology is already making inroads in gaming and can be applied to the travel sector. In gaming, we are seeing the emergence of games called 'play to earn' that allow you to buy game characters and accessories

with cryptocurrency and earn money if you win. The possibility then is to have E-sports and be able to invest in in-game assets. As far as travel is concerned, a luggage tracking service can be offered, keeping track of transports to see if they keep to the scheduled time and if so, automatically warning of any delays. In music, the potential lies in the defence and enforcement of copyright. Finally, the art world is making a lot of headway thanks to the reality of non-fungible tokens*. Works of art thus become digital works that are associated with tokens to represent their originality and ownership, tracing their history all the way back to the last collector who holds them.

3.2 Decentralized financial instruments

Starting with the concept of cryptocurrency, the text then goes on to explain in detail the applications that decentralised finance can have. This elucidation is needed since when it comes to these ecosystems, we no longer use traditional currencies but cryptocurrencies. They have changed the definition of money slightly because they contain special features and, above all, can be used in various applications. Cryptocurrencies are digital currencies that use cryptography in their structure. These coins are in fact created through a system of codes. They function autonomously without being accountable to traditional banking and governmental systems. Cryptography is used to make transactions secure; these coins are different from traditional coins. They can still be bought and sold like other goods. Of the

many cryptocurrencies on the market today, the best known is undoubtedly Bitcoin[48]. These cryptocurrencies have no physical form but can only be stored and traded virtually.

Stablecoins, on the other hand, are digital assets related to the value of a stable currency such as the dollar. They are a middle world between cryptocurrencies and fiat currencies. They are therefore less volatile than cryptocurrencies. They are important because they can be traded one-to-one with the reference currency. An example of a stablecoin is USDC which is linked to the dollar. The value of a USDC must therefore be close to 1 dollar to maintain the 1:1 ratio.[49] The giant Paypal recently opened its gate for cryptocurrencies, this is a great sign from the financial services world.

The so-called De-Fi (decentralised finance) can be defined as an ecosystem of financial applications that are based and work on blockchain technology. The organisation is similar to that of traditional banking services, but the underlying technology (hence its infrastructure) presupposes the absence of hierarchies or at least remains limited compared to the traditional system. An interesting part of this ecosystem are the automatisms. They allow transactions to be carried out automatically without the intervention of third parties, all that is required is that the condition that has been set is fulfilled and that there is an AI reference that can

[48] Bitcoin protocol is explained in the following chapter
[49] Consob, Le criptovalute: cosa sono e quali rischi si corrono

verify this. Automatisms are mainly based on smart contracts. The De-Fi sector exploits various cryptocurrencies and offers many services that will be discussed in more detail later. As this new financial world is continuously developing, it is able to arouse a lot of interest for both investors and creators who are truly passionate about this technology. It is precisely in this way that the environment is constantly expanding in which there is always innovation and a willingness on the part of creators to find solutions to existing problems. The intention of De-Fi is to have exactly the traditional banking services but without the presence of intermediaries, based on cryptocurrencies with open source, permissionless and transparent services. Those who operate financial services on blockchain are in possession of assets. These assets are not controlled by a central authority and can interact with other users directly through peer-to-peer applications, dApps. Finally, unlike a traditional bank, to be operational in De-Fi one does not need to make an application to open an account with anyone, which makes it quick and easy in case one wants to make transactions on public holidays or at inconvenient hours. The ultimate goal is also to make individuals and businesses gain confidence in finance. Trust is a concept on which the whole blockchain philosophy is somewhat based, transparency in this respect could bring positivity in this aspect. Let's focus now on the critical issues of The Finance industry and in a second step, how blockchain technology tries to help. Traditional finance is more prone to an increase in cyber attacks because the technological support for security and risk management is not

present, web criminals are always creating new ways to attack systems and these are not always able to stop them. Related to this is the problem of outdated hardware support systems, in other words there is a poor IT infrastructure. Turning to the subject of transparency, on the other hand, unclear passages can be found when it comes to the use of customers' big data. Moreover, these data are not exploited to their full potential because there are not enough tools. The problem of payment frauds and identity thefts can also be solved with the use of blockchain technology. Traditional finance also has to deal with the time necessarily required for cross-border payments. It can usually take several days and includes bank fees. In addition, there is also the fact that there is a lot of paperwork. All this leads to low customer satisfaction. Decentralised blockchain finance solves purely IT problems due to its advanced IT structure. Thanks to the automaticity of smart contracts, there is no waste of time. There is greater data security due to immutable storage. A cross-border payment can be made in minutes and with much lower fees. Furthermore, since there is no intermediary but smart contracts that function automatically thanks to programming, the problem of trust is solved. The blockchain in fact makes it easier to detect illicit activities. Since transactions are transparent, there is also control over personal data, which are also less likely to be lost because they are protected by ditributed and secured record storage. The applications of De-Fi are varied and include lending, borrowing, payments, insurance, trading (from the

exchange of digitised assets to the exchange of tokens) through decentralised exchanges (DEX), asset menagment, fundraising, savings, etc.

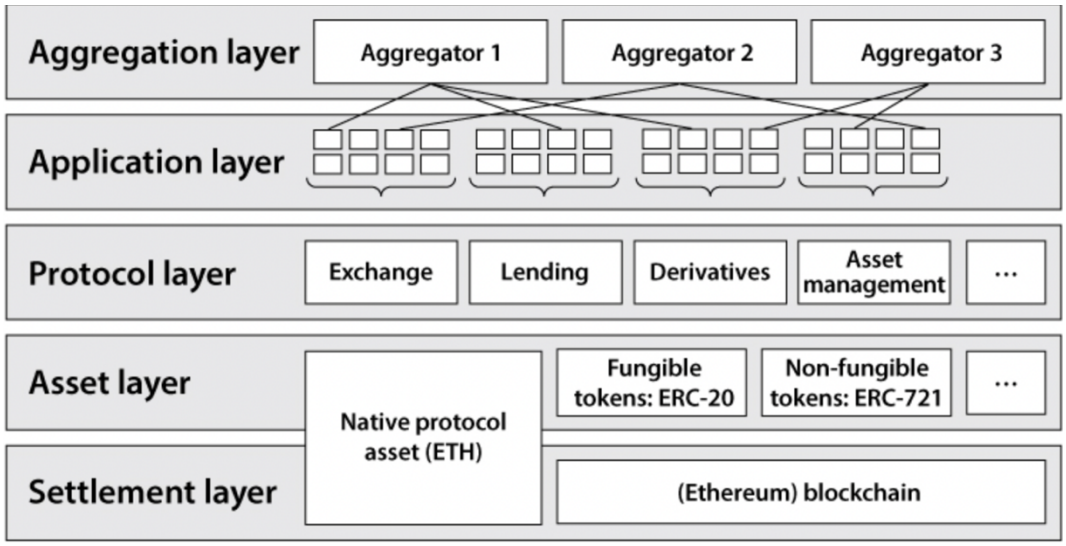
There are various types of protocols that make it possible to lend and borrow crypto-assets. Nobody has to identify themselves. This does not compromise the success of the transaction because smart contracts provide security. If one of the two actors (lender or borrower) should fail to fulfil the terms of exchange, e.g. the borrower should fail to pay the lender, the smart contract would act to cancel the transactions and thus get the value back automatically. This application, like many others, is still experimental given the few years of experience this field has behind it. An example of an important project concerning the landing is Aave, where cash lending in cryptocurrencies takes place.

DEX, on the other hand, refers to Decentralized Exchange. These are real platforms where one can perform the operations of a traditional exchange. The most popular one is Uniswap. Nexus Mutual, on the other hand, is an example of a project dedicated to insurance. Another of the applications listed earlier concerns savings. Savings consists of platforming a sum of money and earning interest from it. An example is Dharma, a platform on the Ethereum and Linen network. Unlike Dahrma, Linen is completely detached from traditional finance and the interest rate is calculated automatically through Compound's algorithm based on the demand for loans and credits.

Finally, it is precisely fundraising that this paper will focus on in the following chapters. It can be argued that in some way crypto finance promotes financial inclusion. In other words, people who for a long period of time have been excluded from access to traditional banking institutions now have the opportunity to engage in transactions quickly, cheaply and without prejudicial obstacles. Although the financial services offered by crypto platforms are more profitable in terms of profit, there is a growing phenomenon whereby consumers are unwittingly taking significant risks through the use of these products. De-Fi is still a relatively new industry, which is why there are certain risks involved. For example, your return on investment may change depending on the dApp you use because it can be subject to volatility[50]. De-Fi has a multi-layered architecture. Each level has its own role and are built hierarchically.

[50] Stepanova, V., & Eriņš, I. Review of decentralized finance applications and their total value locked, 2021

3.6 The De-Fi stack



Source: Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets by Fabian Schär, 2021.

In the figure, we find the various layers, starting from the bottom there are settlement, asset, protocol, application and finally aggregation.

The settlement, layer 1, is what defines what type of blockchain we are using, such as the Bitcoin or Ethereum blockchain as in this case.

Layer 2 is that of Assets. This is where we find the financial assets that can be issued on the settlement layer. In this case, these are tokens, which as we will go into later are mainly developed on the Ethereum network.

In layer number 3, the protocol layer, there are the specific use cases such as decurrency exchanges, debt markets, and asset management. The protocols are interoperable, and this guarantees a high level of customisation.

Level 4, the application level, creates applications through which users can connect to the protocols. In Ethereum these are called dApps.

The last layer, the aggregation layer, is an extension of layer 4. They provide tools for comparing prices or simplifying complex tasks. In fact, different applications and protocols are aggregated together in a way that allows the user to interface with services more easily.

3.3 Considerations from the world

In the global landscape, Switzerland certainly has a very relevant position regarding the development of blockchain. This technology, not only intended to be linked to cryptocurrencies, has a potential that has evidently been recognised by this state. In particular, Switzerland has always been known for its particularity in cyber security, with strict laws protecting privacy, this has served as a basis for the development of new business ideas in the area of Distributed Ledger Technology and blockchain. Switzerland has committed itself to creating a good regulatory basis, a weakness of many other realities that is at the root of all uncertainty among project creators. The institutes of science and technology in Lausanne and Zurich were awarded 'global leaders in crypto education' by Coinbase in 2019. In addition, the first blockchain

professorship university in the world was established in Basel in 2018. Another important aspect is the role the country has gained as events aimed at meetings with qualified people from all over the world such as the Blockchain Leadership Summit in Basel, Annual Blockchain Congress in Geneva, Infrachain in Bern and so on.[51]

So much support from multiple fronts, such as regulatory, educational and finally also application have made this country stand out and made it a benchmark.

With a clear legal framework then, and an aptitude for inclusion and welcoming innovation, the country becomes a real vibrant hub. The city of Zug itself has been called 'Crypto- Valley' but now the term has spread a bit and also includes ecosystems in Zurich, Geneva, Basel, Lucerne, Bern and Ticino. Speaking of the canton of Ticino, the 'Plan B' project in Lugano is one of them.

For some time now, Lugano has been aiming to become a Swiss and European hub for digital innovation. In this sense, the focus on blockchain technology, through concrete projects and solutions, is a strong element in accelerating this process. Under the aegis of its flamboyant LuganoPlanB.

In the immediate future, the city intends to allow citizens and companies to pay taxes, fees and all goods and services in cryptocurrency. Even fines. Lugano will accept Bitcoin, Tether and LVGApoints; it will become one of the first cities in the world to implement a complete cryptocurrency payment system. [52]

[51] Switzerland Global Enterprise, blockchain hub Switzerland, 2020
[52] Planb Lugano web-site https://planb.lugano.ch/?lang=it

The agreement between Lugano and Tether already includes a number of initiatives. Of an educational nature in the field of blockchain and cryptocurrencies, but also to make the city an ideal location for start-ups in need of consultancy services and optimised workspaces. Finally, considering that the creation, mining, of virtual currencies requires the use of significant energy resources related to computer processing, the use of local green energy will be evaluated.[53]

One of the other goals is to get the public administration to develop and deploy blockchain technology for the benefit of citizens. In general, however, Switzerland has no capital gains tax on trading activities, this does not apply to crypto mining and professional trading.[54]

In Europe, the regulatory environment is evolving. On 14 March, the European Parliament's Committee on Economic and Monetary Affairs (ECON) voted on the MiCA (Markets in Crypto-Assets) Regulation. On 31 March, the draft of a new package of anti-money laundering regulations that also cover cryptocurrency transactions was voted on. Two texts that should form the basis of a new regulation of the sector and which will now have to pass the scrutiny of the other European institutions and governments. Referring to Switzerland's comprehensive regulation, Europe has noted how in practice not being efficient at the legislative level brings a number of risks that can no longer be ignored, cryptocurrencies have

[53] Confederazione Svizzera web-site, DLT/ Blockchain, 2022
[54] Switzerland global enterprise, factsheet, la Svizzera come hub della blockchain, 2020

grown into the thousands, and blockchain applications in finance are also expanding. In fact, among the problems with their use, which Europe aims to regulate, are the enormous energy consumption of blockchains. The intent is also to regulate the use to launder money or finance illegal activities. Finally, the absence of stringent consumer protection.[55] Not forgetting the issues of financial stability, given the very wide price fluctuations caused by speculative activities. This is why there has been talk for years of regulating the sector. Often, in fact, attempts have been made to apply existing legislation - often very old - with little results. In this case, therefore, for the European legislator what is important is to guarantee transparency and information on costs and risks, in fact it is in question that the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA) supervise the issuance of certain tokens. With regard to the environmental aspect, however, they are asking the European Commission to take into account the climate impact of cryptocurrency mining.

The new anti-money laundering rules require the collection of information on the origin of the transaction and the identity of the beneficiary. This information will have to be accessible to the authorities. Since there is no minimum threshold for the traceability obligation, all transactions, regardless of amount, will have to be

[55] European Parliament web-site, Cryptocurrencies in the EU: new rules to boost benefits and curb threats, 2022

traceable. In addition, the EBA should set up a register of companies in the sector that are considered high-risk in terms of potential illegal activities. As well as a list of non-compliant providers (service providers)[56]. These should perform a prior check before making funds available to the recipient. That is, checking that the person is not subject to restrictive measures and that there is no risk of money laundering or terrorist financing. On the other hand, the CEO of Coinbase [57] voiced his thoughts on twitter claiming that he does not agree with the EU's wishes. In the tweet Brian Armstrong describes the EU's intentions and finally says: *"These guts all the EU's work to be a global leader in privacy law and policy. It also disproportionately punishes cryptocurrency holders and erodes their individual rights in a deeply worrying way. It is a bad policy.*"[58]

On Wednesday, 9 March 2022, US President Joe Biden signed an executive order that lays the foundation for building a regulatory environment around cryptocurrencies. It is the first executive order issued by the US administration that focuses exclusively on the topic of digital assets and is intended to direct federal agencies to better communicate their work in this area. [59]

---

[56] European Parliament web-site, Crypto assets: new rules to stop illicit flows in the EU, 2022
[57] Coinbase is an exchange. An online platform, through which you can buy, sell and store cryptocurrencies
[58] Tweet of @brian_armstrong 6:18 PM · 30 mar 2022
[59] Executive Order on ensuring responsible development of digital assets, Presidential Actions, march 09, 2022

The goal is to outline six key priorities to protect consumers, ensure financial stability, prevent and combat misuse, ensure leadership of an eventual 'digital dollar', and promote financial inclusion and responsible innovation. President Biden focuses on 'digital assets' that are representations of value, and thus on all CBDCs, i.e. Central Bank Digital Currencies, cryptocurrencies, financial instruments and assets, a credit, a security, a derivative, and in general all those 'assets' that are used to make payments or investments, or to transmit or exchange funds through digital asset exchange platforms, including centralised and decentralised financial platforms. In this order, an approach from all angles is proposed to understand not only macroeconomic, but also microeconomic risks and for each individual, investor or company operating in this sector.

In addition to those mentioned, there are others that are working to enable the development of blockchain technology and the use of cryptocurrencies. These include countries such as Malta, Portugal, Liechtenstein, UK, Dubai, Central African Republic, El Salvador, Costa Rica and Panama. The Central African Republic after El Salvador is the second to have adopted Bitcoin as legal tender. Costa Rica and Panama have turned out to be pro-crypto. Portugal does not tax crypto as long as it is a non-professional activity. Malta, on the other hand, does not tax long-term investments but may do so in minimal terms for short-term ones. Liechtenstein for its part was almost among the first to try to legislate on blockchain. Dubai was among the first to allow trading activities and quickly

became a destination for start-ups. Over time, a community of 'crypto -fans' was created who decided to have a base of operations there.[60]

In March 2022, Dubai established the Dubai Virtual Asset Regulation Law, which aims to be a key player in shaping the future at the legislative level by ensuring transparency and security for investors. The intention is to regulate the use and trading of crypto and other digital assets. The UK in early June brought a crypto bill to congress with the aim of being a starting point for regulation Each nation mentioned in its own way has tried and is trying to find a place for this new technology and integrate it into the system. This need undoubtedly arises for reasons of security and consumer protection given the volume of crypto trading that is taking place and to leave room for innovation.

Chapter 4. Blockchain capital raising

4.1 Tokenomics

4.1.1 Token characteristics

To tokenize means to generate a token and link it to an asset via the smart contract. A transformation and representation of a resource or object occur within a blockchain ledger. When this transformation/link is stored in the blockchain, it is ready to be exchanged.

[60] Tax Planning, I paesi Europei che hanno il miglior regime fiscale per le criptovalute, 2021

The blockchain is capable of revolutionising not only all aspects of finance but also public and civil services. The idea of a tokenized economy, where every form of value storage and public record becomes a token with a fluctuating market value that can be exchanged globally through digital platforms, is plausible.

Tokenization has been used in real estate where the property has been divided into many small shares to be sold to investors in a process of "democratizing" shareholding. Tokenization also has many other applications such as the tokenization of works of art, in the world of sports. Above all, the use of cyber tokens can prove to be most important at the financial level in the stock market sector. Of course, to do this there needs to be a process of converting company shares into tokens.

In this section, we will go into detail about tokens. Mainly we are no longer referring to tokens in general, but to the ones with a financial application part. A token is therefore a set of digital information within a blockchain that confers a right on a given subject. Tokenization is the conversion of the rights of an asset into a digital token registered on a blockchain.

The tokens on Ethereum are created through the implementation of specific smart contracts and can be of different types depending on the type of project for which they are used. If, for example, a token represents a digital currency and a company

share, they will have different characteristics. For these reasons, 'standards' have been created to simplify programming[61].

These standards are nothing more than a set of rules to follow when creating a token, and are called ERC - Ethereum Request for Comment[62]. Creating and customising tokens is relatively simple, and this is in accordance with the guiding principles on which Ethereum is based.

Because tokens are so customisable, it is difficult to list all their properties. It is preferable to bring out what are considered to be the most important aspects. With tokens, if not specified, ownership and possession coincide. For example, to transfer a company share is much easier in the Token Economy than in the traditional one, because you simply need to be able to move that particular token from your wallet to another address. This makes the transaction fast and allows you to sell to the highest bidder anywhere in the world without the need for an intermediary. Another feature is the ease and freedom of implementation. It is possible that even someone with a low level of computer skills is able to create and customise a token. Even if a token belongs to a specific category (we will talk about those later) this does not mean that it cannot have small characteristics that differentiate it from others. Furthermore, we find that the technological universality and the presence of ERCs

[61] The next part will explain the main ones: ERC-20 (fungible token) and ERC-721 (non-fungible token)

[62] In the following chapters they will be explained specifically

make the creation of apps easier in terms of the usability of different tokens. This means that if shares have to be exchanged on Ethereum and tokens from new start-ups have to be added, this is possible without having to change the platform code, due to the ERCs standards.

An important aspect at this point is the classification of tokens under recognisable categories to which regulations can be applied. Classification is not easy, because two tokens with different purposes can be written with the same code. This is why classification is based on functions, rather than by the nature of the token. The basis of the main world classifications act according to the principle of functionality, where two tokens of a different IT nature but with the same purpose of use could fall into one category. The European Union has not pushed forward with legal classifications, but some other countries have. The regulatory frameworks of FINMA and the Swiss Financial Market Supervisory Authority have become the global benchmark. Tokens are therefore divided as: Payment Token, Utility Token and Security Token.

Payment tokens are those that are actually used as payment methods for purchasing goods and services or transferring money. They are also called coins, and capital collections on the blockchain the usage of these types of tokens is called ICOs, Initial Coin Offerings. In contrast, the Utility token is used as a pass to access a digital application, service or content. Spending a utility token would mean accessing one of these functions.

Last but not least there are the security tokens. These tokens are investment tokens, those tokens represent shares in assets. They can represent a claim, or a social right under company law. The token may represent a share, a bond or other derivative financial instrument.

Since the individual token classifications are not necessarily mutually exclusive, it is possible to have tokens that contain features from more than one category and should therefore be qualified as hybrid tokens.[63]

To sum up, the token economy has the power to transform types of security from the real world to the virtual world and to decentralise its control. Tokens have no reason to exist without the blockchain because it is the blockchain that can guarantee transparency, automaticity, the certainty of ownership and decentralisation.

4.1.2 Pros and cons of tokenization

Once the token has been created with the various characteristics of the case, it needs to be circulated. Those who initially support the tokens are the community around them and they believe strongly in the project, without which the tokens would not be of significant value. This is a concept we can find throughout the blockchain

[63] Ferro Lorenza e Massimiliano Maestretti, La tokenizzazione di azioni, tra sviluppi dottrinari e novità normative, 2020

universe; it is the set of people who believe in the functioning of the system that actually makes it work. Furthermore, there is a need to promote the use of these tokens in this community. So that the token economy becomes more dynamic and the network that supports it grows. To do this there is the possibility of mining for example (i.e. giving computational power in exchange for a certain amount of tokens). In any case, the aim is to have a large distribution of tokens in order to ensure decentralisation. Although it would all seem very simple and useful, blockchain and tokenization is not always advantageous. When a company wants to undertake business tokenization, it does so in order to allocate funds for the development of the business, but it has to ensure actually brings benefits. The practice of tokenization can be introduced after a careful analysis in which it is verified that the potential of the business can grow with the implementation. The costs should not be higher or slightly lower than they would have been with a traditional way of raising funds (IPO). Tokenomics therefore also continues this process of analysis to create a valid business model. The hypothesis has to be that tokenization is advantageous, this includes identifying which type of fundraising in blockchain it would be better to operate, in relation to the type of project. [64]

After the decision to carry out tokenomics with a project, two additional types of analysis are carried out: Macrotokenomics and Microtokenomics.

[64] Referring to IEO or STO and ICOs which will be explained later

Macrotokenomic analysis is related to the structure of the token and therefore includes controlling the volatility of the token, being able to guarantee its value and how to have enough liquidity and profitability in the long run of the company. This includes decisions regarding the number of tokens to be issued, the distribution of the token and incentives for investors.[65]

The analysis instead microtokenomics is useful to develop a dynamic asset pricing model of tokens, whose equilibrium value will be determined by aggregating the transactional demand of heterogeneous users rather than discounting cash flows as in standard valuation models.[66]

To get a clear idea, tokenization has advantages such as having a digital representation through the token of any aspect in blockchain, it has the ability to maintain maximum traceability of tokens. The process of tokenization is transparent the tokens are verified, and you can have security of information systems. This helps to counteract the phenomenon of duplication of information. Thanks to its decentralised nature it also guarantees a decrease in costs for the processes that have to manage the projects and reduces the need for intermediaries. Moreover, tokenizing a company remains a less bureaucratic and more streamlined process than the traditional listing process[67]. On the other hand, however, deciding whether

[65] Stylianos Kampakis, Three Case Studies in Tokenomics ,2018.
[66] Cong Lin William, Ye Li, Neng Wang, Tokenomics: Dynamic Adoption and Valuation, 2020
[67] Bit2me academy, cos'è la tokenizzazione? 2020

tokenization is the right choice is a laborious process, and if not properly calibrated there is a risk of making unprofitable decisions. Another negative aspect is the lack of regulation and, as these processes are relatively new, there is always the risk of running into some scam and relying on invalid platforms.[68]

4.2 Development and principal type of tokens

4.2.1 ERC20, Fungible token

The ERC-20 standard identifies the category of fungible tokens. Fungible means that the tokens are interchangeable, they do not have a specific individuality. In fact, this standard is ideal for making digital coins, because they are interchangeable assets of equal value. Each token is equal to another token, in type and value, as for example all 20 euro banknotes have the same value to each other and all 10 euro banknotes are worth 10 euro. In order for a generic token to be compatible with the ERC20 standard, implementations of the token's features are required. There are six features and they are all mandatory: totalSupply, balanceOf, transfer, transferFrom, approve and allowance. In addition, there are some optional ones such as name, symbol and decimal.

[68]Mastropietro Beatrice, La tokenizzazione è una nuova modalità di business, 2021

Table 4.1 Explanation of the six features

FUNCTION	CODE
TotalSupply:	**function** totalSupply() **public** view returns (uint256) *When called by a user, the above function returns the total supply of tokens that the contract holds.*
BalanceOf:	**function** balanceOf (address _owner) **public** view returns (uint256 balance) *When called, it returns the balance of that address's token holdings.*
Transfer:	**function** transfer (address _to, uint256 _value) **public** returns (bool success) ***transfer*** *reallocates tokens from one between users. Here, you provide the address you want to send to and the amount to transfer.*
TransferFrom:	**function** transferFrom (address _from, address _to, uint256 _value) **public** returns (bool success) *The transferFrom function is a handy alternative to* ***transfer*** *that enables a bit more programmability in decentralized applications.*
Approve:	**function** approve (address _spender, uint256 _value) **public** returns (bool success) *With this function, you can limit the number of tokens that a smart contract can withdraw from your balance. Without it, you run the risk of the contract malfunctioning and stealing all of your funds.*
Allowance	**function** allowance (address _owner, address _spender) **public** view returns (uint256 remaining) *Allowance can be used in conjunction with Approve function. When you've given a contract permission to manage your tokens, you might use this to check how many it can still withdraw.*

Source: Binance Academy, An introduction to ERC-20 Tokens[69]

[69] https://academy.binance.com/en/articles/an-introduction-to-erc-20-tokens

The standard stems from the need to have a reference for interoperability and compatibility of tokens in the Ethereum system. Before the ERC-20 was established, the tokens to exchange cryptocurrencies had to build custom 'bridges' of different platforms to support token exchange. ERC20 tokens do not have their own blockchain but they can run on the Ethereum blockchain. ERC20 tokens can be described as a smart contract that runs on the Ethereum blockchain. In fact they are not held by accounts but these tokens exist within smart contracts, this contract has very specific rules for the tokens and is able to associate user balances to the Ethereum addresses they belong to. The smart contract in this case has the ability to distribute tokens, control their movements and balances (if the specific wording in the contract is respected). The main utility is to implement the standard and create a reusable interface for the creation of new tokens. All this is done with an API (application programming interface) which has several advantages for developers. First of all, as already mentioned, it guarantees uniformity in programming, which in turn reduces the difficulty of programming because this API reduces the complexity of the software. This interface is free of charge and this also allows it to be programmed with different programming languages[70]. Furthermore, thanks to the standard there is less difficulty in understanding each new type of token and more security [71].

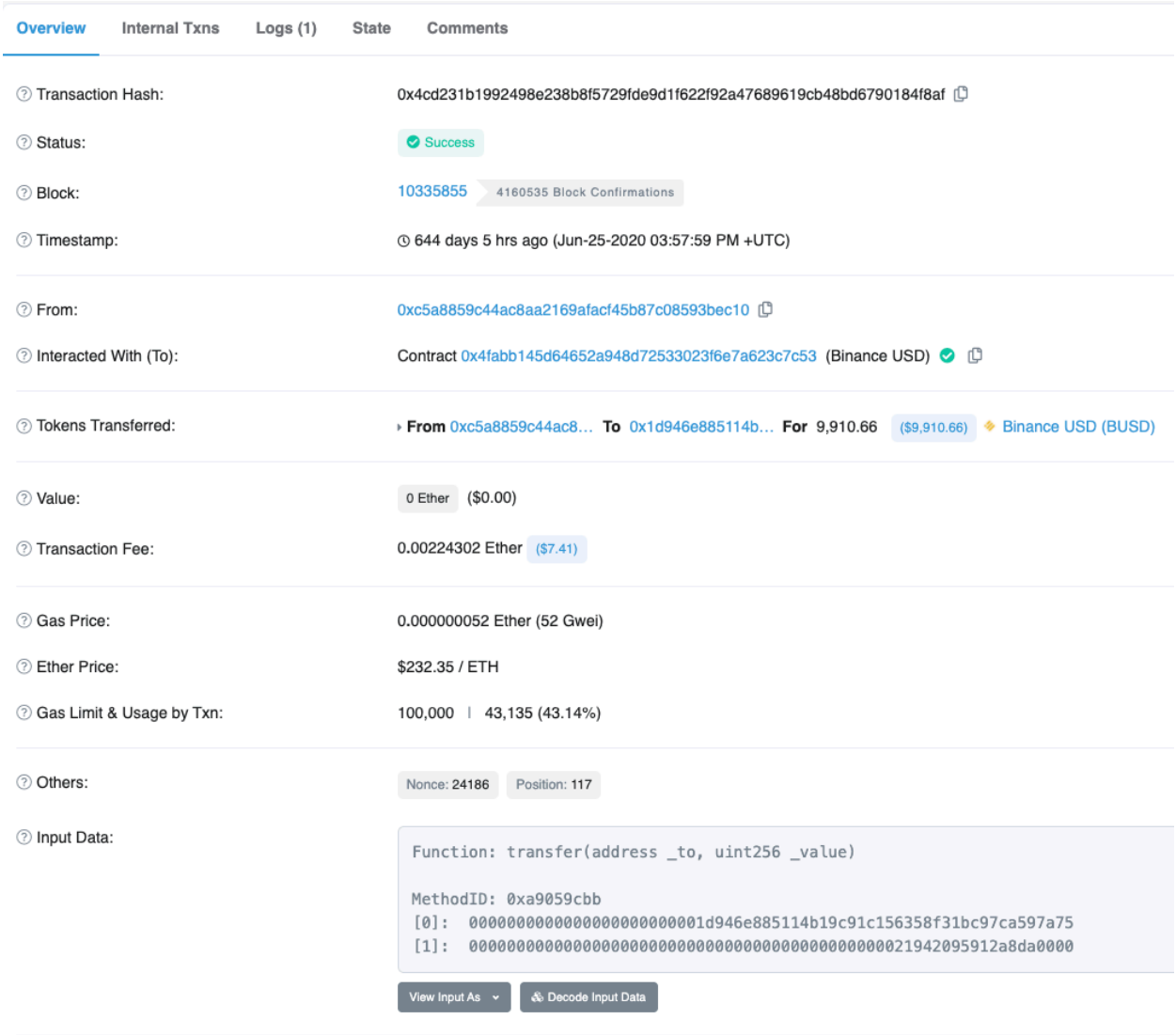
[70] The supported languages are: Solidity, JavaScript, C, C ++, Python, Java and Go
[71] Especially thanks to the token allowance which is explained below

ERC-20 tokens are so widely used because of their adaptability. They have features such as an identifying name and associated symbol, they are capable of managing economic aspects. They manage the interface containing the balances in an address and finally they manage autonomously the withdrawals from an address if permission is given. In the light of all this, explaining how to move tokens in practice could be useful to fully understand its features fully.

To move tokens, users must send a transaction to the contract asking it to allocate some of their balance elsewhere. For example, if Alice wants to send 5,000 BinanceAcademyTokens to Bob, she calls a function inside the BinanceAcademyToken smart contract asking it to do so. Her call is contained inside what appears to be a regular Ethereum transaction that pays 0 ETH to the token contract. The call is included in an additional field in the transaction, which specifies what Alice wants to do - in our case, transfer tokens to Bob. Even though she isn't sending ether, she must still pay a fee denominated in it to have her transaction included in a block. If she has no ETH, she needs to get some before transferring the tokens.[72]

[72] Binance Academy, An introduction to ERC-20 token

Figure 4.6 Example of a general transfer from a wallet to another one



Source: Etherscan[73]

[73] https://etherscan.io/tx/0x4cd231b1992498e238b8f5729fde9d1f622f92a47689619cb48bd6790184f8af

4.2.2 ERC721 Non-fungible token (NFT)

The ERC-721 standard refers to an interface for creating non-fungible tokens (NFTs). These tokens differentiatiate themselves substantially from the ERC20 standard because they are not interchangeable with each other. With this standard it is possible to create tokens that represent digital or physical assets with such particularities that no two are alike. The structure remains the same as that of the other standard but the wording "_tokenId" is added to emphasise the uniqueness of the token. [74]

Function TransferFrom(address_from,addres_to, unit256_tokenId) public.

The ERC-721 standard refers to an interface for creating non-fungible tokens (NFTs). These tokens differentiatiate themselves substantially from the ERC20 standard because they are not interchangeable with each other. With this standard it is possible to create tokens that represent digital or physical assets with such particularities that no two are alike. The structure remains the same as that of the other standard but the wording "_tokenId" is added to emphasise the uniqueness of the token.

One of the earliest usages of this standard was by the Dapp Cryptokitties, each token was associated with a crypto-cat that had unique characteristics and could be resold

[74] Bit2me Academy, che cos'è un token ERC-21? 2020

on the network. Since there were no tokens equal to the others, each one was unique to own. This opened the door to a kind of digital collecting, due to the scarcity of goods with the same characteristics. Apart from this example NFTs can also have many other purposes, for example, to digitally represent a real right (ownership of a property). They are also widely used in gaming and art. An interesting aspect are the applications of these NFTs on virtual realities in applications such as Decentraland, Megacryptopolis and The Sandbox. Since all the information of each NFT is stored, it can be traded transparently in the network and each token has a different market value. All the characteristics that have been listed above in ERC20 also apply in this case but with some differences. The first is that the token is not interchangeable, the tokens are unique and non-uniform and are not divisible. This ERC-721 token also has a name and a definition symbol but does not have the function "allowance" in the structure[75]. Up to date 61659 NFTs have been created, you can see the updated number here: https://etherscan.io/tokens-nft

4.3 Main types of fund-raising on Blockchain

4.3.1 Initial coin offering (ICO)

ICOs are the first of the innovative crowdfunding methods that the Ethereum blockchain has made possible. An initial coin offering (ICO) is a capital raise in

[75] Ethereum web page, standard token non fungible ERC-721, 2022

which investors fund a project in exchange for tokens. These tokens can be classified as 'coins' (payment tokens). Since 2013, many ICOs have been launched worldwide by start-ups. The project is usually presented in the so-called 'white paper', in which all the details of the project are explained, as well as technical and legal aspects and how it is intended to be carried out. It is obvious that the more a project is described in detail, the more credibility investors will give it. The white paper contains information about the type of project, the ultimate goal, how much money is needed to realise it, how many tokens the founders are holding, in which currencies tokens can be bought and how long the campaign will last.

Investments can usually be made in both fiat currencies and cryptocurrencies. Before this stage, however, those who want to raise capital determine what structure their ICO will be. Statistic supply and static price is when the company sets the maximum goal, and the total amount of token supply is determined, and the token is worth a specific price. As a second category there is the static supply and dynamic price, in this sense the founding goal is not fixed, and it is on this that the price of each token will depend. Finally, there is the dynamic supply and static price, where the amount of funds determines the size of the supply.

These projects are still not fully regulated but progress is being made. In 2017/2018 there was no regulation whatsoever and therefore one relied only on the white paper to decide whether or not to invest in a project, and there was a possibility that it was risky. As soon as the investor has received the token, the token can be used as a

means of payment on the project platform. Otherwise, the token can be sold. The sale can be made to the highest bidder in order to get the profit between the purchase and sale costs. The possibility of reselling tokens has meant that there is a great deal of interest, and this has led to a great volatility in asset values. Why ICOs have been so incredibly successful has been due to the simplicity of the transaction. It was possible to operate without detailed documentation and was therefore a simplification compared to the usual regulated crowdfunding, this also gave a timing advantage. The simplicity of programming smart contracts, thanks also to the existence of the standards mentioned above, allowed even those who were not familiar with the sector to develop their project. In addition, the very low costs for collections and the possibility of being able to raise funds from all over the world meant that many projects were launched. What was created was the so-called 'FOMO' or fear of missing out. This concept implies sometimes irrational choices to follow the actions that most people do around us. It is also a very interesting phenomenon observed in behavioral finance.

However, the ICO phenomenon has not been as successful as expected. In a way, it can be said that the same points that made ICOs successful were also the ones that made them fail. When smart contracts are written by non-competent people, they can contain errors, and it has been easy for malicious computer scientists to take advantage of these errors. In addition, the costs over time have increased as well as regulation in some parts of the world has been advanced and this no longer

gives the green light as easily as in the early days. Undoubtedly with the possibility of regulating these aspects, the blockchain reality has many advantages to carry out this type of capital raising. IEOs (initial exchange offerings) and STOs (security token offerings) are also types of capital raisings but with different characteristics that will be mentioned in the next sections.[76]

4.3.2 Initial exchange offering (IEO)

Initial Exchange Offerings (IEOs) are capital raisings, like ICOs, that are matched by the issuance of crypto assets but, unlike ICOs, are conducted directly within a crypto asset exchange.

In a statement dated 14 January 2020, the SEC points out that these exchanges [77]are not registered on official registries. However, exchanges act as intermediaries between companies seeking capital for their projects and investors. For this reason, they are encouraged to carry out due diligence. Legally, exchanges are not obliged to check whether a project is reliable or not, but their reputation is affected. As is the case with stock exchanges in order not to lose credibility in the eyes of investors. Binance which is one of the largest exchanges in the world makes sure not to propose failed projects because it would pay in terms of visibility. According to the

[76] Initial Coin Offering, Invest, 2022

[77] Cryptocurrency exchanges (including Binance and CoinBase) are platforms on which it is possible to buy and sell crypto assets of all kinds, such as the well-known cryptocurrencies

2019 data with respect to the geographical areas where the IEOs have been used the most, it shows that 85% of the total is concentrated in the United States, Estonia, Singapore, South Korea, Honk Kong and United Kingdom.[78]

In fact, these countries are the ones that have immediately shown interest in the technology and have tried to regulate it. In this scenario, Italy is trying to work on a regulatory framework. Consob's final report "Initial Offerings and Crypto Assets Exchange "of 2 January 2020 contains guidance on the subject of capital raisings using blockchain technology. It is possible to make an IEO in the official crowdfunding portals that are registered with Consob. This report emphasises the importance of transparency and that all information about the token and the project must be made available to potential investors. In addition, the scope of IEOs has been reduced to crowdfunding with utility tokens as this is a regulatory grey area. Consob's proposed approach therefore seeks to recognise crypto assets that are different from the financial instruments set out in Article 1(2) of the Consolidated Law on Finance and from the investment products set out in Article 1(1) (w-bis.1), (w-bis.2) and (wbis.3). In Italy, as in other parts of the world, the direction is to define the requirements for classifying the raising of capital through coin (ICO), utility (ITO) and security (STO). The term IEO identifies the collection through an exchange.

[78] Coinmarketcap.com

In IEO, investors can buy assets before they start trading in the open market. It is the exchange that arranges for their users, registered through the KYC[79] (know your customer), to buy assets with the identification of potential investors. In order to get on the exchange, the project needs to have a solid foundation like a team of people experienced in the field, a solid business model and a profound white paper, as mentioned earlier. Another aspect to take into consideration when starting the project is the decision between having a hard cap and a soft cap. The hard cap puts a limit on the amount of money that can be invested while the soft cap has an initial capital target to reach but if there are still investors they will be accepted anyway.[80] Unlike ICOs, there is an intermediary, lower costs for publicising the project (the exchange will do this), and attention to minimum regulation which is now the responsibility of the exchange rather than the project founder. An important innovation is the almost automatic listing of assets on the market, the implementation of this service by the exchange that manages the secondary market of the crypto asset increases its liquidity. The negative aspects inevitably remain, however if care is not taken one could run into misuse of funds by the founders, the possibility that the exchange is not entirely independent of the founders increases

[79] With KYC you lose the anonymity discussed in the previous sections, this is because it is not the user who keeps the keys public, private and has his own wallet but lets the exhange do it for him.
[80] Binance Academy, What Is an Initial Exchange Offering (IEO)? 2022

the risk. Compared to IPO (Initial Public Offering), the IEO has no amount of initial capital on the part of the token issuing company. [81]

Chapter 5. Finding procedures for equity projects in Blockchain

5.1 Security token offering (STO)

Unlike ICOs, STOs distribute tokens that can be represented under the status of 'securities' and are related to investment activities. These tokens are called security token and are financial instruments, fungible and exchangeable because they have a monetary value attached to them. They are considered a step ahead of ICOs precisely because of the securities that constitute the token. Indeed, STOs are considered a solution with a focus on regulatory compliance. The goal is not to put the investor in a dark position where he has shortcomings compared to the project owner. The token type in STOs guarantees a pre-programmed revenue stream and contains rights and obligations. These tokens are traded on specialised exchanges because they are subject to regulatory compliance checks, including an analysis of the project and the various related procedures. STO launch platforms seek to assist companies with their processes, token issuance and regulatory approach. The main ones include Polymath (POLY), Securitize, Harbor and Swarm. STOs have the

[81] Furnari Salvatore Luciano Cosa sono le Initial Exchange Offering. Vantaggi e rischi di un nuovo strumento di cripto-finanziamento, 2020

advantage of transparency, all transactions and compliance can be monitored and they have more credibility than ICOs due to the history of fraud and legislation. Not to be underestimated is the great improvement in timing compared to the issuance of traditional securities and their slow and costly management due to an old infrastructure and the presence of intermediaries. Timeframes are also linked to costs, which are significantly lower than traditional ones. Programmability is an advantage as these tokens can be applied directly by smart contracts. The STO market has no geographical boundaries. The timing of operations is also different from traditional ones as they are closed at weekends while digital assets are active at any time of day throughout the year. Token security also opens the door to divisibility. Real estate or works of art can be accessible to those who do not have the opportunity to invest because it allows them to divide the value. A work of art worth 2 million euros could be tokenised into 4000 units of 500 euros. This brings a greater possibility of liquidity and accessibility. The security token is therefore a cryptographic token linked to an offer of securities.Opposite to the other tokens (utility and coin), this is the only one that offers investors an actual stake in the company. They are therefore regarded as investment opportunities. Utility and Coin tokens function respectively as, the former, serving a specific purpose, such as the possibility of entering an ecosystem, and the latter, as an exchange value.

To be classified as security, a token must possess some general characteristics.[82] In ordinary shares, the security token identifies the minimum unit of participation in the capital of a company; there must be a share-token correspondence, i.e. each security token must correspond to one ordinary share. The owner of the security token also has the right to vote in relation to his share of the total. The vote is digitally represented by the underlying technology. Having this type of token also gives the right to receive profit when the shareholders decide to distribute the profit. This payment could also be automated through smart contracts. Since the token is re-saleable, it is possible to have a capital gain from the process of buying and selling. The liability remains limited to the amount of capital that has been invested and furthermore, there is a residual right of bankruptcy in case of bankruptcy. With the security token the legal ownership of the token can be verified in the blockchain and its value is directly related to the valuation of the company.

5.2 ICO, IEO, STO: the comparison

In this section we can directly find the differences between the various types of capital raising. Referenced are macro areas such as the nature of the token, the legislative aspects that regulate or do not regulate tokens, what concerns the

[82] Tokens representing ordinary shares.

ownership of the company/start-up after the issuance of these instruments and the risk protections linked to the profits that may accrue to the investor.[83]

Between ICOs, IEOs and STOs, the difference that first jumps out is the differences of the nature of the tokens. In the ICO we find a coin token, while utility or coin token in the IEO, and finally a security in the STO. The legislation around these three modes can be divided into two parts: the unregulated aspect which concerns the issuance of coin tokens or utilities, and the regulated aspect which includes the security one. The legislative context impacts not only on the founders of the company, at the level of decision-making and discernment of the tokens, but also and above all on the investor's risks and eventual profits. It goes without saying that it is very important to study the characteristics of the project through the white paper. It will be from this that there will be a better understanding about the profit opportunities. For the token coin and utility, there is not a recognized interest connected to the change of the value of the company therefore the investor knows that he will be able to obtain profit only through the difference between the price of sale and that of purchase. If one refers to security tokens it is necessary to make the distinction between stock and bond.[84]

When the token represents a share, the investors not only gain from the appreciation of value of the asset, but they will also participate in a possible division of the profit

[83] Deloitte, Security token offerings: The next phase of financial market evolution?
[84] This thesis will not deal with bonds but with shares.

at the end of the financial year. In the case of a bond token, investors are entitled to periodic interest, again depending on the characteristics of the particular token.

We can summarise the characteristics schematically as follows:

Table 5.2 Technical and regulatory context

	ICO	IEO	STO
TOKEN	Coin	Coin or Utility	Security
Issuing platform	Start-up Web site	Exchange	Exchange for STO
Secondary exchange platform	Start-up web site,	through Exchange or free trade wallet	Exchange for STO
Current regulatory framework in the EU	No one	No one	MIFID II
Future expectations of the EU regulatory framework	European Parliament Regulation, Council on market of crypto-asset	European Parliament Regulation, Council on market of crypto-asset	MIFID II updates

Source: Own elaboration according to D'Andreta, Security Token Offering, 2021

Table 5.3 Founders' point of view

	ICO	IEO	STO
Effect on start up property	No one	No one	Equity: fractional ownership
bureaucratic obligations	No one	What the Exchange require	drafting of informative prospectus, Anti money laundering[85]

Source: Own elaboration according to D'Andreta, Security Token Offering, 2021

Table 5.4 Investors' point of view

	ICO	IEO	STO
Token expendability	Payment method	use/access to a service (utility), Payment method (coin)	Equity: voting rights
Investor role	Grant investor	Grant investor	shareholder
Investor rights	No one	No one	Dividend share, voting rights
Return on investment	Appreciation asset (sale)	Appreciation asset (sale)	Appreciation asset sale and dividends
bureaucratic obligations	-	-	Know your customer procedure [86]

Source: Own elaboration according to D'Andreta, Security Token Offering, 2021

[85] In the event of an investigation, they must be able to provide evidence certifying that this fact did not occur

[86] Investors will be identifiable through this procedure that allows to link an investor to a real person through his/her personal information / documents

5.2.1 STO Vs IPO

The comparison between Security Token Offering STO and Initial Public Offering IPO is still a bit premature, but it aims to show the main differences between the regulatory, technological, and economic realities.

Table 5.5 Differences between STO and IPO

	Security Token Offering	**Initial Public Offering**
Asset	Stocks or bonds represented by tokens	Shares
Eligible companies	Startup	SMEs and large corporations that meet certain capital and income requirements
Purpose of raising	Realize an innovative project of the startup	Consolidate your position and expand into new industries or foreign markets
Regulation	MIFID II	MIFID I + Regulation of Markets organized and managed by Borsa Italiana S.p.A.
Bureaucratic requirements	Simple and verified by the Exchange	Complex and verified by Borsa Italiana S.p.a.
Timelines	Short terms (1-3 months)	Long terms (6-9 months)
Costs	Low	High
Primary marketplace platform	STO Exchange	Stock exchange
Secondary marketplace platform	STO Exchange or decentralized Exchange	Stock exchange
company that manages the assets	Management is totally decentralized on blockchain	Monte Titoli
secondary market liquidity	currently slightly liquidity	Quite of liquidity

Source: D'Andreta, Security Token Offering, 2021

5.3 SECURITY TOKEN CHARACTERISTICS

5.3.1 How to create a security token

From a technical point of view, there are solutions like standards, that can be used for the creation of a security token, and thus facilitate the process of tokenisation of corporate shares. The most widely used generic standards for tokenisation classified as security are: ERC-1450, and ERC- 1462. In addition we have a standard that is not generic but specific to the tokenization of shares: EIP-884.

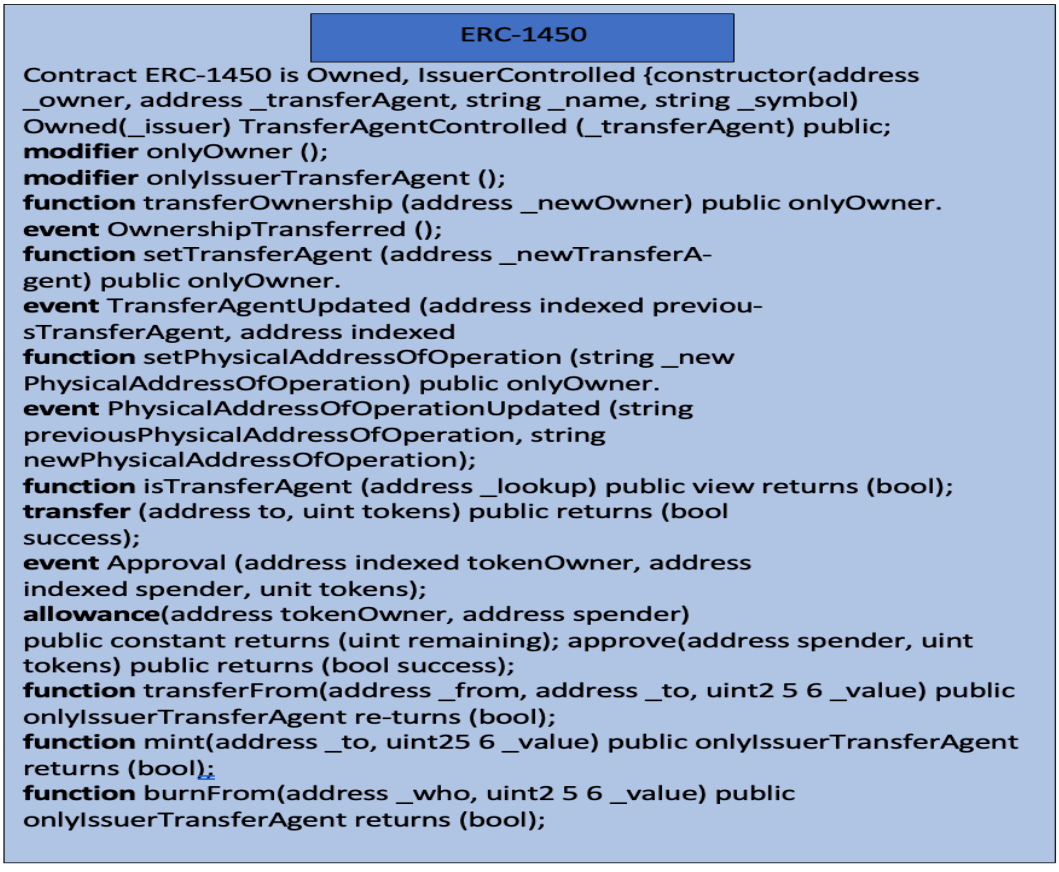
The ERC-1450, was created on 25 September 2018 by John Shiple, Howard Marks and David Zhang. It allows the creation of tokens and also their exchange. It complies with the Regulation Crowdfunding, Regulation D and Regulation A. In addition, the KYC and AML processes are taken into account.

These features extend those of the ERC-20, which is designed to create fungible tokens. Among the additional features, there is the management of the registration and transfer of security tokens. For legal value in the smart contract that builds the token must be present the Issuer, the RTA[87], and the name and symbol of the token. The Issuer of the security is the one who has to create and connect the RTA, ensuring the KYC and AML activities. In the event that the RTA loses its privatekeys, there is a function that allows the USER to reassign the role of the RTA. For the SEC there are legal requirements to be met such as the RTA must

[87] RTA- Registered transfert agent entity that can perform certain functions of the smart contract.

have certain requirements: the investor's name, Ethereum address and securities. The balance must be kept off-chain and the SEC must be able to access them. In addition, a certain discretion must be respected for investors' personal information, so it cannot be recorded on the blockchain. Here we see the code in order to create the token, that must be present in the smart contract in order to comply with the rules of the US SEC. This is the code that needs to be included in the contract in order for it to be a security token of the ERC-1450 standard.

Figure 5.6 Example of standard command ERC-1450



Source: D'Andreta, Security Token Offering, 2021

Another example of a standard Security token is the EIP-1462 from authors Maxim Kupriianov and Julian Svirsky released on 1 October 2018. This token is used as a standard because it respects the Know Your Customer (KYC) procedure and the anti money laundering (AML) legislation worldwide. It is also an extension of the ERC-20 and the changes are closely following the KYC and AML guidelines. There is a possibility of blocking this token if any legal disputes occur. It is also possible to attach documents directly in the smart contract that constitute the token. The types of documents can be individually modified and vary from country to country. The feature of inserting external documents and the fact that it is not programmed like the previous one only for American regulations, allow you to take advantage of its versatility by being able to adapt it to the many different national regulations.

Figure 5.7 Example of standard command EIP-1472

EIP-1472

```
contract BaseSecurityToken is IBaseSecurityToken, ERC20 I
struct Document {
bytes 3 2 name;
string uri;
bytes 3 2 contentHash;
}
mapping (bytes3 2 => Document) private documents;
function transfer(address to, uint25 6 value) public returns (bool) {
          require(checkTransferAllowed(msg.sender, to,
 value) == STATUS_ALLOWED, "transfer must be allowed");
          return ERC20.transfer(to, value);
}
function transferFrom(address from, address to, uint25 6 value) public returns (bool) I
          require(checkTransferFromAllowed(from, to, value _
= STATUS_ALLOWED, "transfer must be allowed");
          return ERC20.transferFrom(from, to, value);
}
function _mint(address account, uint2 5 6 amount) internal {
          require(checkMintAllowed(account, amount) = =
STATUS_ALLOWED, "mint must be allowed");

ERC20._mint(account, amount);
I
function _burn(address account, uint2 5 6 amount)
internal t
          require(checkBurnAllowed(account, amount) = =
STATUS_ALLOWED, "burn must be allowed");
          ERC20._burn(account, amount);
I
function attachDocument(bytes 3 2 _name, string _uri,
bytes3 2 _contentHash) external f
          require(_name.length > 0, "name of the document
must not be empty");
          require(bytesCurplength > 0, "external URI to the
document must not be empty");
           require(_contentHash.length > 0, "content hash is
required, use SHA-1 when in doubt");
          require(documents[_name].name.length == 0, "document must not be existing under the
same name");
          documents[_name] = Document(_name, _uri,
_contentHash);
I
function lookupDocument(bytes3 2 _name) external
view returns (string, bytes3 2) f
          Document storage doc = documents[_name]; return (doc.uri, doc.contentHash);
byte private constant STATUS_ALLOWED = 0x11;
function checkTransferAllowed (address, address, uint256) public view returns (byte)
          ( return STATUS_ALLOWED;
}
function checkTransferFromAllowed (address, ad-dress, uint256) public view returns (byte)
           { return STATUS_ALLOWED;
}
function checkMintAllowed (address, uint256) public view returns (byte)
          {return STATUS_ALLOWED;
}
function checkBurnAllowed (address, uint256) public view returns (byte)
          {return STATUS_ALLOWED;
  }
}
```

Source: D'andreta M., Security Token Offering, 2021

As a third type the EIP-884, by the author Dave Sag, was released on 14 February 2018. This standard is tailor-made to represent corporate shares complying with the Delaware General Corporations Law (DGCL). Like the others it is also an extension of the ERC-20 but in addition this standard can also be used for the implementation of ERC-721 of non-fungible tokens (NFT). The state of Delaware, in its DGCL in Title 8, was one of the first to expressly enact regulations allowing shares in a company to be tokenized with blockchain. Thanks to this token, STOs similar to Initial Public Offerings (IPOs) can be carried out, but without the need to rely on a traditional stock exchange. Here we also find compatibility with SEC requirements for crowdfunding. In order to have full legal effect, a token that is used as a share in Delaware must still have certain characteristics such as, the KYC[88] process as a list of shareholders specified in parts 219 and 220 of the DGCL, contains certain information as explained in sections 156, 159 and 218 of the DGCL. Shares must be transferred following the references in section 159 of the said document. Each token must correspond to a single share which must be recorded as fully paid. Finally the legislation requires a way to recover the tokens, in case of a lost private key, in order to delete the old Ethereum address and have a new one with the restoration of the shares held.

[88] Know your customer

Figure 5.8 Example of standard command ERC-884

ERC-884

```
contract ERC884 is ERC20 [
event VerifiedAddressAdded(
        address indexed addr,
        bytes32 hash,
        address indexed sender
        );
event VerifiedAddressRemoved(address indexed addr, address indexed
sender); event VerifiedAddressUpdated( address indexed addr, bytes32
oldHash,
bytes32 hash,
address indexed sender
);
event VerifiedAddressSuperseded(
        address indexed original,
        address indexed replacement,
        address indexed sender );
function add Verified(address addr, bytes32 hash) public;
function removeVerified(address addr) public;
function updateVerified(address addr, bytes32 hash) public;
function cancelAndReissue(address original, address replacement) public;
function transfer(address to, uint2 5 6 value) public returns (bool);
function transferFrom(address from, address to, uint2 5 6 value) public
returns (bool);
function isVerified(address addr) public view returns (bool);
function isHolder(address addr) public view returns (bool);
function hasHash(address addr, bytes32 hash) public view returns (bool);
function holderCount() public view returns (uint);
function holderAt(uint25 6 index) public view returns (address);
function isSuperseded(address addr) public view returns (bool); function
getCurrentFor(address addr) public view returns (address);
}
```

Source: D'Andreta, Security Token Offering, 2021

In Italy there are still no standards and start-ups performing tokenization not following a precise regulatory framework. As a minimum requirement MIFID II and also Consob's equity crowdfunding regulation have to be taken into account. Although this regulation does not contain the guidelines to be applied in blockchain, it contains all of the obligations that both authorised portals and start-ups as well as small and medium-sized enterprises must comply with when raising funds by issuing securities. The platforms on which to raise funds are the traditional equity crowdfunding platforms, that have already been authorised by Consob. In Italy, there are two cases of platforms operating with the exchange of security tokens: Opstart, an equity crowdfunding portal in partnership with SEED Venture is working on the tokenization of fundraising and Equito. The latter does not currently have a Consob-authorised portal but intends to join the blockchain world with STOs. Finally, it can be assumed that a hypothetical ERC, compliant with Italian and European regulations will be implemented as a standard in the future, based on MIFID II and will closely follow current and future Consob regulations.[89]

5.3.2 Emission token phases

The token issuance phase can also be identified as the primary market phase. The tokenization of shares is the step preceding the raising of capital on the blockchain

[89] Ethereum Improvement Proposal, EIP-1450: ERC-1450 A compatible security token for issuing and trading SEC-compliant securities

and executed via smart contracts. Immediately afterwards, the public offering of tokens should take place as follows, as suggested by a recent report by Deloitte.[90]

In step 1, the orientation, a group of target investors is identified and targeted information is gathered. This information can be the business plan, capital needs and profit expectations. In general, the information required to be reported to act legally may differ depending on the state and platform where the tokens and thus the STOs are launched. To give an example, in Europe if you do not exceed a certain amount of capital you do not need a legal prospectus. In the United States of America, less comprehensive documentation may be submitted.

The second step refers to the design of the offer. This is where we structurally delineate the tokens, the quantities, the offer and its duration while also considering the rights attached to it. In addition, it is necessary to keep in mind the legislation where we are operating. We arrive at the third step by deciding which platform to entrust the launch to. Platforms can offer different services such as a wallet where tokens are kept. In addition, a reliable service provider has to be appointed to safeguard all the underlying operations such as storing the cash flows and trading the token. Then as a fourth step arises the raising of capital, with marketing activities and approval by the authorities. Finally as the last step Listing of security on the trading venue page 15 of the Deloitte document. The platforms themselves

[90] Deloitte, Security token offerings: The next phase of financial market evolution? Pag. 14

may also have listing rules. In Italy, it is necessary to apply, for access, to the portals authorised by CONSOB[91]. These portals must be registered in the Equity Crowdfounding register and also require many of the documents mentioned above and some additional ones such as: Relevant accounting information, information about the governing body and resumes of all directors, tax treatment of investments and various information about costs or fees that are for investors.

Once approved, the token can be developed directly in the portal or an already developed token can be imported. A token is considered already developed when the deployment of the smart contract in Ethereum has taken place. The next step is, as explained above, a marketing campaign that can bring in investors. Marketing is not only pre-launch but also during. It can continue in fact by publishing the approaching or exceeding of targets or by keeping the amount collected up to date. After the token is issued, there is a second smart contract that determines how the money is collected. The gathering of capital itself is also regulated via smart contracts, it is much more efficient and transparent than traditional means. In addition, the fundraising can only take place with Ether in Ethereum, an exchange of currencies is subtended, which can be for example the exchange from Euro to Ether. Once the public offering of tokens is over, the company can dispose of the collected funds and the investors can then take advantage of the rights acquired

[91] M. D'andreta, Security Token Offering, 2021

through the shares. The shareholders now own the token and can dispose of it, in fact, direct sale via secondary markets is possible. In the event that the collection does not reach the set limit or fails for some reason, the smart contracts will make sure to return what is owed to the buyers in their wallets.

5.4 Legislation: MIFID II, Security Act and Howey Test

The relevant question remains the identification of the security token according to the regulations in force in the various countries of the world. When it comes to something fundamentally new, precise regulation is lacking, but somehow the general law must be respected. To identify which one has to be complied with, it is useful to look at the regulations of issues in the traditional markets. As far as the US is concerned, the Security Act and the Howey Test have been taken as references. In the EU the Markets in financial instruments directive - MiFID II is applied. Usually, one starts by understanding what the different states' understanding of "security token" is. For the USA the definition of a token in the Security Act of 1933 does not specify the particularities that a 'security' must have, but the investment contracts that fall into this category such as: equities, bonds and derivatives on equities and bonds. Since the written paper or digital form is not specified, it is not the nature of the asset that classifies it as a security but rather its economic-financial function. To determine whether a token represents an investment contract between two parties, however, we do not use the Security Act,

but the Howey Test. It refers to a 1946 U.S. Supreme Court case that states that it is an investment contract if "*a person invests money in a joint venture for the purpose of deriving reasonable profits from the employment of other persons."*

Applying the Howey Test therefore means checking whether the principles contained correspond to those in the token[92]. All the criteria that have been explained and cited in the judgment therefore form what is now known as the Howey Test. It therefore verifies the presence of an investment of money that is in a common enterprise with a reasonable amount of profit expected and that it derives from the commitment of third parties. The investment is then assessed in its substance rather than in its form. After the token has been declared as a security under this test, there are further rules to follow. These rules concern the token in the first place, but also the collecting companies and the issuing (primary market) and exchange (secondary market) platforms. Regarding the European panorama, the reference is to MIFID II. In Europe, there is no definition of a token that can be classified as 'security'. Instead, there are a series of characteristics that if possessed by the token make it identifiable in the category of financial instrument. Thus, among others, the following are considered financial instruments: Transferable securities, money market instruments, option contracts, derivative financial

[92] Embroker business advice and research, What Is the Howey Test & Does Crypto Pass? | The 4 Elements, 2022

instruments for credit risk transfer. This European MiFID II regulation is superordinate in the hierarchy of sources and sets a uniform regulation for national authorities. This stipulation therefore does not allow states to make their own classification regarding this issue and in the final report "Initial offers and cryptocurrency exchanges" of Consob is explicitly explained in paragraph 2.1. The criterion of economic-financial function is therefore maintained without looking at the technical characteristics of the token. In addition to looking at security tokens, regulation of the other two categories of tokens and their possible applications is also in the pipeline. The European Commission has in fact published a “Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets” considering the objectives of regulations for the grey areas of certain crypto-assets, the development of DLT projects through standards and competitiveness in the sector, and the protection of investors and consumers. In the Occasional Papers of the Bank of Italy "Economic and Regulatory Aspects of Crypto Assets", some definitions and distinctions between tokens based on economic (not legal) categories are given. In fact, it speaks of class DT1 referring to "virtual currencies" ("crypto-assets" without rights or liabilities), DT2 representing digital coins or payment tokens, DT3 regard security/asset tokens and finally DT4, utility tokens/ consumer tokens.[93]

[93] Banca D’Italia, Questioni di economia e finanza, Occasional Paper, 2019, Pages 10-11

Looking at the big picture, in Italy some steps have been taken with the simplification decree number 135 of 14 December 2018 art.8. Unfortunately, it has not been completed anymore and is therefore lacking guidelines for specific DLT and Smart Contract identifications. To get an idea of the situation in other countries, Switzerland can be taken as an example, which is a pioneer in the pursuit of the innovation wave especially in the Zug area and has been named 'Crypto Valley'. The Swiss Financial Market Supervisory Authority (FINMA) sets out how it will handle applications for ICOs on the basis of current financial market law. In its assessment, FINMA follows an approach focused on the economic functions and purpose of the tokens. For this reason, the issues of token classification and also negotiability and transmissibility are very important. For these reasons, FINMA distinguishes and clearly describes three types of tokens: utility tokens, asset/security tokens, and payment tokens.

5.4.1 Regulation around the world with examples of STO projects

In order to get a general overview regarding this type of technology in the world, the following are examples of STO realities.

In Japan, an amendment to the Act on Settlement of Funds and the Financial Instruments and Exchange Act (FIEA) was implemented in 2019, which sought to define the security tokens and define the cryptocurrencies that are to be used to purchase them and as investments in a broad sense. However, there is no real

specific regulation, it goes on to follow the rules of a regular Initial Public Offering (IPO).

In Nigeria, a very particular initiative was implemented in 2020: the Nigerian SEC declared any token as security, but this limits the distinctions and the possibility of other categories developing.

In Luxembourg, the "Blockchain Bill" was enacted in 2020, allowing the issuance and circulation of security tokens registered on an "electronic secure system" on the primary and secondary markets respectively.

In 2021, Switzerland enacted the Swiss DLT Regulation, which sets a global benchmark in the fintech-blockchain sector. Within this framework, there are some interesting innovations with regard to the tokenization of company shares. In fact, a new class of tokens called "Uncertificated Register Securities" is defined. They are assets that represent the company shares with legal effectiveness. To have this classification they will have to respect certain rules specified in the DLT Regulation. In addition, a Security Token Exchange licence has been defined that authorises the listing and exchange of shares on blockchain for start-ups.

Liechtenstein, on the other hand, was one of the first countries that with the " Blockchain Act " in 2019 managed to develop a regulatory framework specifically for security tokens, ICOs and STOs. In this law, the "Token Container Model" can be found. This model explains precisely the processes of tokenization of assets or rights, which have the same legal value as traditional off chain process. Moreover, it does not only takes the Ethereum blockchain[94] into account, but Blockchain technology in general. This openness allows greater flexibility for future regulation updates and can be easily used for future protocols.

A practical example of STO in Liechtenstein is that of NASH (neon exchange). The token issued is called NEX, the issue took place on Ethereum and ended with a raised amount of 25-000-000 dollars. The STO was authorised by the FMA, the Financial Market Authority of Liechtenstein. The issued token has some peculiarities but is still part of the security tokens according to the country's Blockchain Act. Nex acts as a profit-sharing arrangement. As one of the first, a team of 20 lawyers, experienced in international law combined with expertise in distributed technologies worked on this project.

[94] In this context, it is the one considered most for the type of fundraising activities because it currently remains the main

Moving to Europen Union instead, we have the example of Neufund in Germany, with an ERC-20 token called Neumark. It had a target raising of $1,312,399.36 and eventually raised $4,410,560.00. Its STO was one of the first to be authorised in the European Union by a national authority. Germany's BaFin (The Federal Financial Supervisory Authority) has allowed this fundraising to go ahead, but with a minimum investment of $100,000 to protect investors. Neufund was created with the aim of becoming a European platform for STOs and Equity Token Offerings whose ownership is divided among the token holders. So far, despite several projects and millions of dollars raised from around the world, the start-up has blocked the operation of the platform due to the unclear regulatory framework. CEO Zoe Adamovicz explained on social media that, despite several requests, BaFin has never given full legal effect to their platform and therefore to the collection of projects. In this case technology and legislation did not go hand in hand, caused problems regarding the operation.

Conclusions

Considering the blockchain technology in general, it has the potential to open up many possibilities in various areas. It is certain that it can provide a very high quantity and quality of data and information. The main problem the technology is currently facing is that in each sphere, one must be able and ready to process it. Looking at the purest version of the blockchain technology, it would seem that we

are therefore heading towards an automated world where everything is considered and calculated upstream.

With a society open to the adoption of technology, it is more reasonable to think that there will be a co-existence between blockchain technology and the traditional way the world is working with today. The figure of the intermediary, for example, does not have to completely disappear but can simply change and adapt its role with respect to the service that the market will require.

What we know so far is that this is a technology that is currently discovering its full potential and is still developing. It is difficult to predict some of the trends that we will have in the short to medium term, given the continuous radical innovation in the sector. This, however, does not exclude the fact that many of the existing applications do not have the basis for them to be rediscovered and repurposed over time. As more and more users are becoming interested in the world of blockchain, we can imagine how greater knowledge leads to a proportionally faster improvement. Although with regard to De-Fi, one can point out the basic characteristics that are leading a large number of users to use it (security, transparency, convenient interest rates), it is impossible to predict future developments at present. One point in common with all the applications of various macro-areas is the security that in order to be able to make the best use of the technology, a commitment to information and above all training is necessary.

Traditional methods of finance, investment, data processing/management and so on have limits, limits that in an increasingly globalised, borderless and increasingly digitised society are beginning to be too restrictive. The steps forward that are being taken, the usefulness and optimisations that are possible are opening the door to a revolution that, although it seems to be underway now, is probably still holding much in store for us in the future.

This is confirmed by the attention that institutions are showing on the subject and the attempt to legislate on it. With the study of technology and an integration with the traditional, one can have the tools to optimise resources.

The purpose of this thesis was to give the necessary tools to a company that wants to consider entering into a STO. The operation of security tokens and their increasing use lead us to emphasise their added value compared to traditional practices. In a secondary market hypothesis, we know that the trading hours would not be limited as in classical STOs, but 24/7. The possibility of interoperability that from Ethereum for instance will allow in the future to have assets of a different nature in one portfolio, this would mean having global liquidity in common. Security tokens offer an entirely new and efficient way of splitting a high-value asset. In this way, it is indeed possible to fractionate an asset into large amounts and see the possibility of having a diversified market portfolio. Exchanges such as NASDAQ and NYSE have a very slow process of ownership transfers compared to an Ether or Bitcoin transaction which occurs within minutes and so also the transfer

of ownership is almost immediate. Thanks to blockchain, the ownership shares that will be tokenized will have an inherent advantage: the capital tables will be updated automatically. This leads to a massive decrease in administration costs. As far as the compliance of tokens is concerned, this can be scheduled, which means a decrease of barriers in the sale of cross-border securities. What we can expect in the near future is that the securities design space will evolve in its inherent characteristics. Noteworthy is that design development does not remain the same for everyone. It is important to have a clear idea of the project being developed. Only by knowing the various facets and what value and rights to attach to the token, one is able to recognise the best path to take between ICO, STO or IEO.

More specifically, then, some enabling factors emerge for companies to undertake an STO. The first is the need for preparation for raising capital, by the creation of a business case followed by the writing of the whitepaper. At this stage, consultants can help assess the feasibility of the initiative. A financial advisor, together with a lawyer help formulate the offer. At this design stage, a decision is also made on which blockchain to operate on, the platform in this case having to be able to support the features one wants to give the token. The next step is to identify financial service providers such as brokers and payment providers. This is followed directly by the capital-raising phase where a marketing campaign is put in place to gain attention from possible investors. Finally, there is the possibility of listing on appropriate stock exchanges. Possible platforms for tokens are InvestaX, MERJ

Exchange, openfinance and tZERO. According to Forbes reporting some statistics of the STO secondary market in 2021, the total trading volume is around $69,660,511.35. According to the STO marketplace Area2Invest, the global market is growing. In fact, it is projected to increase by 56.9% annually reaching $3 billion in 2025 [95]. The tZERO CEO said that the high initial development expectations for security tokens have not been fully met, but nonetheless it is still nothing decisive because there have been changes between 2019 and 2020. In fact, in the tZERO platform there were 5 million traded in 2019 versus 54 million in 2020. The possible cause of the lower than expected trend may have been the slow and uncertain regulatory vision as well as the market adoption took some time. Therefore, for the future we expect that also thanks to clearer legislation there will be real cooperation among new ways of doing finance. Whether it is cryptocurrencies, stablecoins, smart contracts and security tokens in blockchain a good implementation with the current system can benefit both realities by making them more streamlined, (as far as traditional services are concerned) and more real (for blockchain realities) thanks to the regulations that are coming out on the topic and the volume of money already invested in.

[95] Coin Desk, Security Token Market Shows Signs of Resurgence, 2021

Bibliography

Antonopoulos Andreas, Mastering Bitcoin, 2017

Antonopoulos, Andreas M., and Gavin Wood. Mastering ethereum: building smart contracts and dapps. O'reilly Media, 2018.

Aslam, Javed, et al. "Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry." Journal of Innovation & Knowledge 6.2 (2021)

Attico Nicola, blockchain guida all´ecosistema, 2018

Attico, Nicola. Blockchain. Guida all'ecosistema. Tecnologia, business, società. goWare & Guerini Next, 2018.

Banca D'Italia, Questioni di economia e finanza, Occasional Paper, 2019

Banotra, Atul, et al. "Use of blockchain and internet of things for securing data in healthcare systems." Multimedia Security. Springer, Singapore, 2021. 255-267.

Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake" ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34-37, 2014.

Biden, Executive Order on ensuring responsible development of digital assets, Presidential Actions, March 09, 2022

BitFury Group, Public versus Private Blockchains, 2015,

Bonomi Carlo, Assolombarda, Il futuro della blockchain, 2021

Buterin (2015a)

Buterin, Ethereum white paper, 2014

Carboni Davide. Dagli smart contract alle ICO. Immunotable. today, 2017.

Casey Michael and Wong, Global Supply Chains Are About to Get Better, Thanks to Blockchain, Harvard business Review, 2017

Coin Desk, Security Token Market Shows Signs of Resurgence, 2021

Coletti, P., 'Bitcoin's baby: blockchain's 'tamper-proof' revolution', 2015

Comandini Gianluca, Da zero alla luna, 2020

Cong Lin William, Ye Li, Neng Wang, Tokenomics: Dynamic Adoption and Valuation, 2020

Consob, Le criptovalute: cosa sono e quali rischi si corrono
Conway Luke, Blockworks, Proof-of-Work vs. Proof-of-Stake: Which Is Better? February 2022

Crosby et al., Blockchain Technology: Beyond Bitcoin, 2016

Daian P., R. Pass, and E. Shi, "Snow white: Provably secure proofs of stake," Int. Assoc. Cryptolog. Res., Tech. Rep. 2016/919, Sep. 2016.

Deloitte, Security token offerings: The next phase of financial market evolution?
Derose, C., Blockchain for Beginners -Behind the Ingenious Security Feature that Powers the Blockchain, 2015

Embroker business advice and research, What Is the Howey Test & Does Crypto Pass? | The 4 Elements, 2022

Evans David, "Economic aspects of bitcoin and other decentralized public-ledger currency platforms." 2014

Fahad Saleh, Blockchain Without Waste: Proof-of-Stake,
Ferro Lorenza e Massimiliano Maestretti, La tokenizzazione di azioni, tra sviluppi dottrinari e novità normative, 2020

Fiedler Ante, Lennart, and Ingo. "Cheap signals in security token offerings (STOs)." Ante, L. & Fiedler, I.(2020) Cheap Signals in Security Token Offerings (STOs). Quantitative Finance and Economics 4.4 (2020)

Furnari Salvatore Luciano, Cosa sono le Initial Exchange Offering. Vantaggi e rischi di un nuovo strumento di cripto-finanziamento, 2020

Gates, Mark. Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. CreateSpace Independent Publishing Platform, 2017.

Irresberger et al. The Public Blockchain Ecosystem: An Empirical Analysis, 2020
Kampakis Stylianos, Three Case Studies in Tokenomics ,2018.

King and Nadal, Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012
Makoto Yano, Blockchain and Crypt Currency, 2020, chapter 5

Mastropietro Beatrice, La tokenizzazione è una nuova modalità di business, 2021
Misra, P., "5 Ways blockchain technology will change the way we do business", 2018

Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System
Nguyen C. T. et al.: Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks 85731C. T. Nguyen et al.: Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks 2019

Oliveira Luis; Zavolokina, Liudmila; Bauer, Ingrid; Schwabe, Gerhard University of Zurich, To Token or not to Token: Tools for Understanding Blockchain Tokens, 2018

Pilkington, Blockchain Technology: Principles and Applications, 2016

Stepanova, V., & Eriņš, I. Review of decentralized finance applications and their total value locked, 2021

Swan Melanie, Blockchain- Blueprint for a New Economy, 2015

Switzerland Global Enterprise, blockchain hub Switzerland, 2020

Whitfield Diffie And Martin E. Hellman, New Directions in Cryptography Invited Paper, 1976

Word bank Group, Distributed Ledger Technology (DLT) and Blockchain, 2017
Zatsarynnyi, Kostiantyn. Security Token Offering: legal issues. Diss. Mykolo Romerio universitetas, 2020.

Zibin, Shaoan, Hongning, Xiangping, & Huaimin, Blockchain challenges and opportunities: a survey 2017

Sitography

https://academy.binance.com/en/articles/an-introduction-to-erc-20-tokens

https://academy.binance.com/it/articles/a-beginners-guide-to-security-tokens

https://academy.binance.com/it/articles/what-is-a-blockchain-consensus-algorithm

https://academy.binance.com/it/articles/what-is-an-initial-exchange-offering-ieo

https://academy.bit2me.com/it/cos%27%C3%A8-token-erc-721/

https://academy.bit2me.com/it/cos%27è-un-danno/

https://academy.bit2me.com/it/que-es-tokenizacion/

https://blockworks.co/proof-of-work-vs-proof-of-stake-whats-the-difference/

https://brightnode.io/it/tokenizzazione-delle-aziende-nuovo-modo-per-finanziarle/

https://cryptonomist.ch/2022/03/10/ordine-esecutivo-biden-mondo-crypto-esulta/
https://ee.stanford.edu/~hellman/publications/24.pdf

https://en.cryptonomist.ch/2022/03/09/us-biden-signs-executive-order-cryptocurrencies/?_gl=1*n55f5y*_ga*NTI0MzAzNi4xNjU0NjM5MDQz*_ga_JZ46NG4KVG*MTY1NDY3OTc4MC4yLjEuMTY1NDY3OTc4MS4w

https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_White_Paper_-_Buterin_2014.pdf

https://ethereum.org/it/developers/docs/standards/tokens/erc-721/

https://ethereum.org/it/developers/docs/standards/tokens/erc-721/

https://etherscan.io/tokens-nft

https://etherscan.io/tx/0x4cd231b1992498e238b8f5729fde9d1f622f92a47689619cb48bd6790184f8af

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

https://fchub.it/cosa-sono-le-initial-exchange-offering-vantaggi-e-rischi-di-un-nuovo-strumento-di-cripto-finanziamento/

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8746079

https://library.oapen.org/bitstream/handle/20.500.12657/37713/2020_Book_BlockchainAndCryptCurrency.pdf?sequence=1#page=88

https://novitafiscali.supsi.ch/945/1/Maestretti%26Ferro_La%20tokenizzazione%20di%20azioni%2C%20tra%20sviluppi%20dottrinari%20e%20novit%C3%A0%20normative.pdf

https://planb.lugano.ch/?lang=it

https://planb.lugano.ch/?lang=it

https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-andsmart-contract-based-financial-markets

https://www.assolombarda.it/servizi/ricerca-e-innovazione/documenti/libro-bianco-il-futuro-della-blockchain

https://www.bancaditalia.it/pubblicazioni/qef/2019-0484/QEF_484_19.pdf

https://www.bitpanda.com/academy/it/lezioni/qual-e-la-differenza-tra-utility-token-e-security-token/

https://www.bitpanda.com/academy/it/lezioni/qual-e-la-differenza-tra-utility-token-e-security-token/

https://www.blockchain4innovation.it/criptovalute/blockchain-cosa-sono-i-protocolli-pow-e-pos-e-a-cosa-servono/

https://www.blockchain4innovation.it/criptovalute/token-cose-come-viene-utilizzato/

https://www.coindesk.com/markets/2021/06/22/security-token-market-shows-signs-of-resurgence/

https://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1

https://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1

https://www.consob.it/web/investor-education/criptovalute

https://www.cybersecurity360.it/legal/criptovalute-ordine-esecutivo-di-joe-biden-sugli-asset-digitali-impatti-privacy-e-security/
https://www.embroker.com/blog/what-is-the-howey-test-does-crypto-pass/

https://www.europarl.europa.eu/news/it/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats

https://www.europarl.europa.eu/news/it/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

https://www.findlaw.com/consumer/securities-law/what-is-the-howey-test.html

https://www.focusrisparmio.com/news/azimut-ragnatela-fintech-alternativa-alle-banche

https://www.focusrisparmio.com/news/blockchain-qui-per-creare-valore-non-per-disintermediare

https://www.focusrisparmio.com/news/martinelli-gimme5-cresciamo-nel-digitale-grazie-alla-blockchain

https://www.investopedia.com/tech/2018-year-security-token/

https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

https://www.mercati24.com/ethereum-classic-vs-ethereum-differenze-vantaggi-opinioni/

https://www.millionacres.com/real-estate-investing/crowdfunding/regulation-d-explained-what-are-regulation-d-offerings-in-real-estate-crowdfunding/

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2018-12-14;135

https://www.novasera.it/quali-sono-le-differenze-tra-criptovalute-e-token/#Cose_un_token

https://www.s-ge.com/it/publication/factsheet/svizzera-come-hub-della-blockchain

https://www.s-ge.com/sites/default/files/publication/free/factsheet-blockchain-switzerland-s-ge-en-2020-12.pdf

https://www.sif.admin.ch/sif/it/home/finanzmarktpolitik/digitalizzazione-settore-finanziario/blockchain.html#:~:text=Il%201%C2%B0%20agosto%202021,della%20piazza%20finanziaria%20%C3%A8%20essenziale.

https://www.solofinanza.it/15042019/che-cose-la-tokenizzazione/16387

https://www.taxplanning-internazionale.com/miglior-regime-fiscale-per-le-criptovalute/

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

https://www.zora.uzh.ch/id/eprint/157908/1/To%20Token%20or%20not%20to%20Token_%20Tools%20for%20Understanding%20Blockchain%20Toke.pdf

https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/audit/deloitte-cn-audit-security-token-offering-en-201009.pdf

https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/audit/deloitte-cn-audit-security-token-offering-en-201009.pdf

https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/audit/deloitte-cn-audit-security-token-offering-en-201009.pdf