POLITECNICO DI TORINO

Master Degree in

Engineering and Management

Master's Thesis

How DLT can improve the IPO value journey for companies and investors

Relatori
prof. Marco Cantamessa

Candidato
Danilo Santorsola

A.A. 2018/2019

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

One of the most interesting technologies, which has become more and more famous in recent years, is undoubtedly the Distribute Ledger technology, more commonly called blockchain. This is a constant trending topic when it comes to digitization and innovation in the financial world. In this study will be analyzed, in particular, an application of this technology to a particular and important financial process, the IPO. Since January 2009, the date of Bitcoin's debut, to date, blockchain technology has certainly grown and improved. What was once considered almost as one transitory trend, is now almost ready to revolutionize many industries, to the point that the company will probably recognize a pre- and post-blockchain historical period.

At first, the blockchain was simply the technology that supported Bitcoin. It was already a small revolution as it introduced various innovations such as: decentralization of currency and financial transactions, decentralization of data and information, elimination of the need for "trusted" third parties to verify transactions, resistance to censorship, immutability and inability to corruption and introduction of the Proof of Work consent method, which makes the blockchain unique in combining the power of computational processing through the use of nodes connected to the network. These nodes verify all transactions and ensure the functioning of the entire network, as explained below in this paper.

After a short time, some experts have found that the blockchain could have different use cases than the just bitcoin. Furthermore, Bitcoin's blockchain was not able to fully meet certain expectations at the time, such as being able to create smart contracts, and that's where Vitalik Buterin's character comes in. A Russian Canadian programmer, he noticed that Bitcoin's blockchain was limited and could not scale enough. Vitalik then decided to do it all by himself and, in 2014, he put together the Ethereum project. Ethereum was an important evolutionary step in blockchain technology, which introduced some expansions and improvements. Ethereum and other similar projects like NEO, EOS, TRON, are known as distributed virtual machines as they can run decentralized applications on their blockchain. All of this is analyzed

and explained in this thesis, so to provide the reader, the degree of understanding necessary to analyze the more technical aspects of the applications of these technologies. Ethereum also made it possible to lower average transaction costs and make micro-payments more easily. Moreover, considering the potential of Ethereum and the possibility to run applications on its blockchain, the concept of digital resources tokenized, and not fungible tokens was introduced. These changes allowed the blockchain to become a more commercial platform through the concept of distributed virtual machine. Vitalik has also created decentralized organizations (DAOs), decentralized companies based entirely on smart contracts.

Despite the rapid development and implementation of DLTs, some problems persist over time and represent the obstacles that technology finds on its way to full adoption in the real world. For example, the problem of scalability remains: Bitcoin can handle about 7 transactions per second while Ethereum from 15 to 20. Visa can support up to 24,000 transactions per second. Much more important numbers and, to this day, difficult to reach by any reliable blockchain solution. Fortunately, the extreme interest of experts and enthusiasts and the great potential of the blockchain now known by everyone, have allowed to develop interesting solutions to improve scalability, such as *Lightning Network*[1] for Bitcoin and *Plasma*[1] for Ethereum. As explained in the following chapters, sidechains offer another solution. Through them, for example, you can transfer a tokenized asset on a secondary network, so as to keep free the main blockchain that can handle multiple transactions.

Today the blockchain is probably very similar to what was Internet in the 90s. We are still in the early stages, but it may not be long before it reaches many aspects of our daily lives. The adoption and knowledge of this technology is still in its beginnings but fortunately the situation is improving month by month.

[1] Lighting Network and Plasma born respectively in 2015 and 2017, by Thaddeus Dryja, Joseph Poon and Vitalik Buterin. Plasma and Lightning Network were both proposed as scaling solutions for blockchains and each of them has its own mechanisms and particularities which will be not analysed in this paper since those are not necessary for the purpose of this paper.

In fact, in the last few years many projects have been born that allow to issue generic assets on the blockchain and consequently various scenarios have been opened in the financial field on what could involve the issue of tokens that represent real assets.

One of the most interesting scenarios includes the Security Tokens and consequently the Security Token Offering (STO), focus of this thesis. The roots of this idea are not too far from those of the blockchain itself and also come to life in the "effervescent" ecosystem of Silicon Valley.

Hardware companies, famous for their initial capital expenditures and high bankruptcy rates, had long been able to circumvent the venture capital road by using crowdfunding as a capital raising strategy. With the launch of the Bitcoin idea and soon after Ethereum, platforms were created that allowed to raise capital in the same way used by the existing crowdfunding platforms, but through the issuance of tokens. Each token represented the right to use, once developed, the platform that provided the service sold. As with the large hardware companies, the Initial Coin Offerings (ICOs) allowed the raising of capital for service/software companies through DLTs. Blockchain technology and smart contracts allowed token buyers to claim ownership of these digital assets/virtual currencies without the involvement of a third party to act as an accountant to avoid double spending.

Initially, companies were able to raise millions in a very short time by showing only a theoretical "white paper" and little or no progress on a real product. In this unregulated area, the cost of capital from raising money using service tokens was significantly cheaper than raising money through the traditional equity route. With any opportunity for profit in an unregulated industry, unscrupulous personalities can turn to the amateur consumer. With the increasing frequency of "scam" projects that have not delivered the product described in their white papers, the CFTC and SEC in the US have taken a more active position and increased supervision of the industry and the ICOs.

From here it took little to create real security tokens, which would represent a security on the blockchain via tokens. Despite the enthusiasm and increasing regulation by the authorities, it is not easy to replace an entire financial world, based on principles and rules that have been

present for many years and refined over time, with a new fully digitized system and without trusted third parties. Nevertheless, the increased liquidity of the security tokens, pushes companies that are now considering the possibility of raising funds using STOs.

In the classic way of raising capital, however, especially for companies that want to open up to the public market, there are many aspects of the raising process that add value to the company and that are mainly brought by intermediaries who take part in the process. The growth of a company and of its intrinsic value during an IPO is the perfect example.

Is it therefore really convenient to eliminate these intermediaries? Is there a real reduction in costs and technical time? Can the introduction of blockchain technology in capital raising processes have the same impact both on companies that decide to list themselves on the stock exchange and on those that want to raise capital privately?

To better explain and understand how the DLT can bring benefits in the IPO processes, in the second chapter of this thesis will be exposed and explained both topics trying to report as fully as possible all the key aspects of the two major topics.

This paper has been used to look for answers to these questions and has done so by analyzing what has been implemented so far and the possible future scenarios developed by those who are most in contact with this technology and the processes of raising capital. This has been done through qualitative research, more specifically through the analysis of the understanding and opinions of experienced individuals interviewed.

Furthermore, it is proposed a comparison between a current IPO and a potential IPO process after the application of the new technology.

Finally, the analysis of the voices of a significant sample of professionals (from consulting firms, investment banks or active in the blockchain world) together with the opinions sought in the meagre literature present at the moment, have contributed to the result of this research work, which findings have been reported in the last chapter.

2. LITERATURE REVIEW

The purpose of this chapter is to present the research area, the problem statement and hypotheses necessary to face the problem addressed by this paper. The following paragraph will help the reader to have a clearer idea of the distribute ledger technology, and in particular of the application of it to the security world. The remaining paragraphs explain the ambiguity which surrounds the security definition, the classic IPO process and its value chain.

2.1 DISTRIBUTED LEDGER TECHNOLOGIES

There is a problem which flummoxed computer scientists for decades: The Byzantine Generals Problem. A group of generals each commanding a portion of the Byzantine army, encircle a city. They must decide whether to attack or retreat. But whatever they decide, the most important thing is that they reach a consensus. But consensus is difficult to reach because the general in this army, as people in the real world and in the online world, can't trust each other. A general might say they plan to attack, when he actually plans to retreat. Just one dishonest general means everyone else dies in battle. The general had no choice but to route all of their battle plans through a central authority. That is also why a website like Amazon needs to check people's data with the banks to be sure people are good for the money they promise to pay. Hence, especially in the online world, a third party is needed to store and verify everything.

Let us abandon the famous problem just mentioned for a moment and focus on today's world. The internet, today, filled up the gap of trust with huge parties represented by companies such as Google, PayPal, Airbnb. More generally, the traditional transaction paradigm requires that two users who want to exchange an asset, such as money, rely on a central authority called Trusted Third Party. This body has the task of recording the transaction history of all users of the network, so, at any time, the status of the system can be reconstructed. Let's take as an example a payment by credit card: the two users must go through the bank that on the one hand ensures that the user who transfers money has the financial means to do so and on the other hand that the transaction is successful. The presence of this central body is

necessary to ensure that the service works properly, but in this way, the trusted third party itself has all the power and this creates a single point of failure.

In 2008 Satoshi Nakamoto (pseudonym) proposed a solution to these problems and to The Byzantine Generals Problem, proposing the first blockchain, able to guarantee transactions in Bitcoin without the need for the guarantee of a central body [3]. Combining, in an original way, some established technologies (encryption and communication between nodes), Nakamoto presents the first completely decentralized peer-to-peer (P2P) exchange network that allows users to exchange money directly without going through any kind of financial institution (Trusted Third Party). Thinking back to The Byzantine Generals: if their orders were recorded on the blockchain, as it is explained later on in this paper, each general would have a copy of other generals' battle plans, always up-to-date and 100% verified.

It must be specified that the term "Bitcoin" indicates both the currency that is exchanged and the protocol that manages the system; it should also be noted that the Bitcoin protocol defines a blockchain, not the blockchain (intended as technology) in general.

Since the Bitcoin protocol is open source, anyone can modify the protocol and create their own version. As a result, thousands of altcoins (alternative crypto-currencies) have emerged, trying to be a faster, more anonymous or more efficient form of Bitcoin [4]. Moreover, it was soon realized that dwelling only on currencies is highly reductive, since blockchain technology allows to decentralize the transactions of any digital asset. The benefits of the new technology are disruptive: it has the ability to replace any entity that centrally controls a network or system [2].

Compared to the traditional paradigm, this technology requires that all the nodes that are part of the network have a copy of the transaction history, thus making it accessible to all in a direct and transparent way, as shown in Figure 1. Furthermore, the protocol ensures that the copies of the ledger in the hands of the different nodes are consistent with each other and that it is not possible to deceive the system by recording untrue transactions or by modifying the transactions already consolidated in the register. Therefore, this emerging technology ensures that no node can behave opportunistically in relation to others, that there is no censorship or

exclusion and guarantees also, with an extremely high level of reliability, the accuracy of the data [5].

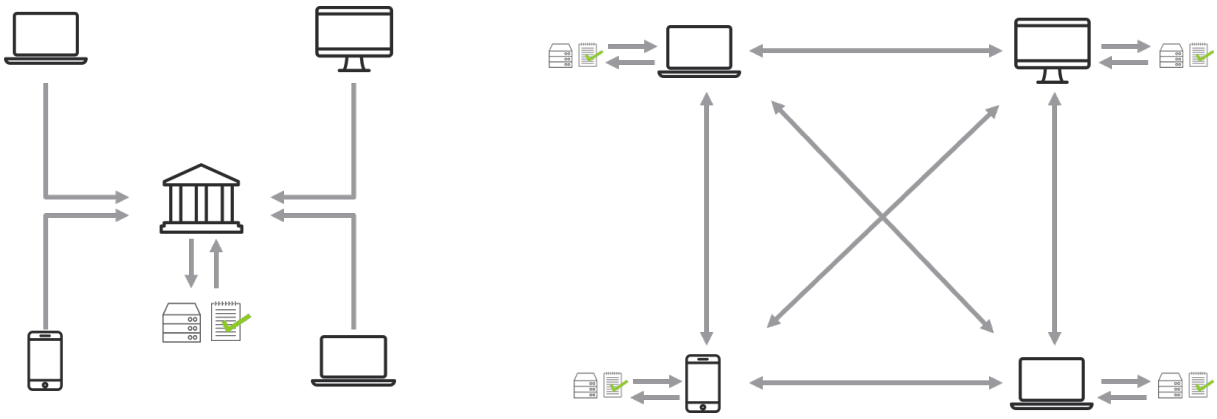

FIGURE 1 : NETWORK WITH A CENTRALIZED AUTHORITY VS. DISTRIBUTE LEDGER NETWORK

In the contemporary panorama, many types of blockchains have arisen, which vary among them since they offer different solutions to the common problem of the decentralization of power between the nodes. Buterin[2] proposes a three-dimensional trilemma: all blockchains can never excel in all the three aspects, and therefore they must make compromises between them [6]. The three dimensions are:

- **Decentralization**: defined as the ability of the system to function in a scenario where each node has only $O(c)$[3] resources
- **Scalability**: defined as the ability to process $O(n)^2 > O(c)$ transactions
- **Security**: defined as resistance to attacks by groups with $O(n)$ resources

For example, a blockchain network such as Bitcoin uses a consensus algorithm that renounces scalability in exchange for decentralization and security, while a network managed by a central body is scalable and secure but, by nature, it is not decentralized. Most of the blockchains in development today are somewhere between these two forms, based on the qualities they

[2] Vitaly Dmitriyevich "Vitalik" Buterin is a Russian-Canadian programmer and writer primarily known as a co-founder of Ethereum and as a co-founder of Bitcoin Magazine.

[3] *c* is the magnitude of the computational capacity, while *n* is the "order of size" of the system

renounce to have, for example private blockchains focus on efficiency and security leaving out the decentralization of the system [7].

2.1.1 THE TECHNOLOGY

As mentioned above, the special feature of the technology under consideration is to decentralize the control of the transaction register. Doing this means creating a network of nodes that all have the same power and rights over the register (also called ledgers). Compared to the classic client-server logic, a peer-to-peer (P2P) network requires that each node functions both as a client and as a server and contributes equally to the provision of network services.

It's better, however, to first take a step back and analyze the concept of ledger. The ledger represents a register of all transactions carried out in the past by users on the network. This is essential to ensure transactions and to reconstruct the current status of users. The simplest example is the bank account: the institute in fact allows the user to spend money only if his balance allows it, to carry out this check it is therefore necessary to retrace all its income and expenditure. The classic scenario is the one in which the ledger resides on the server of the Trusted Third Party and users declare the intention to make a transaction in favor of another. The central body listens to the communication, verifies the formal correctness and the possibility of making the transaction, and writes it on the ledger.

The first problem to deal with in a network (such as the DLT one) is that the communication of the transaction has to be not altered in any way. To do this, the technique of digital signature is used. The user who wants to send the money (or any other type of asset) defines a message with the amount, address of the recipient and unique code of the transaction and signs everything with his private key. In this way, all the nodes that receive it can immediately verify the integrity of the message and the authenticity of the sender through the corresponding public key (this presupposes that the private key-user correspondence is guaranteed) [5].

With this new technology, the ledger is no longer kept and updated only by the central authority but is saved locally by each node belonging to the network. In the next paragraphs it is explained how these ledgers are updated so that they are always the same among them, now the issue of the role of nodes is addressed.

On the theoretical side, therefore, each node should save a copy of the ledger on its device and consequently all nodes would be on the same level. However, on the practical side, this activity requires a huge amount of storage space that the commonly used devices are not able to offer. In practice, therefore, there will be two levels of nodes: the "**full**" ones and the "**light**" ones [8]. The full nodes represent the structure that supports the entire network, only among them is in fact distributed the transaction log. The light nodes represent instead a lower hierarchical level, able only to consult the ledger, and to communicate with the full nodes through a protocol of client-server type. The result is a system that is not completely distributed, but rather decentralized, i.e. a hybrid between the centralized and the distributed. This difference can be seen intuitively in figure below (Figure 2).

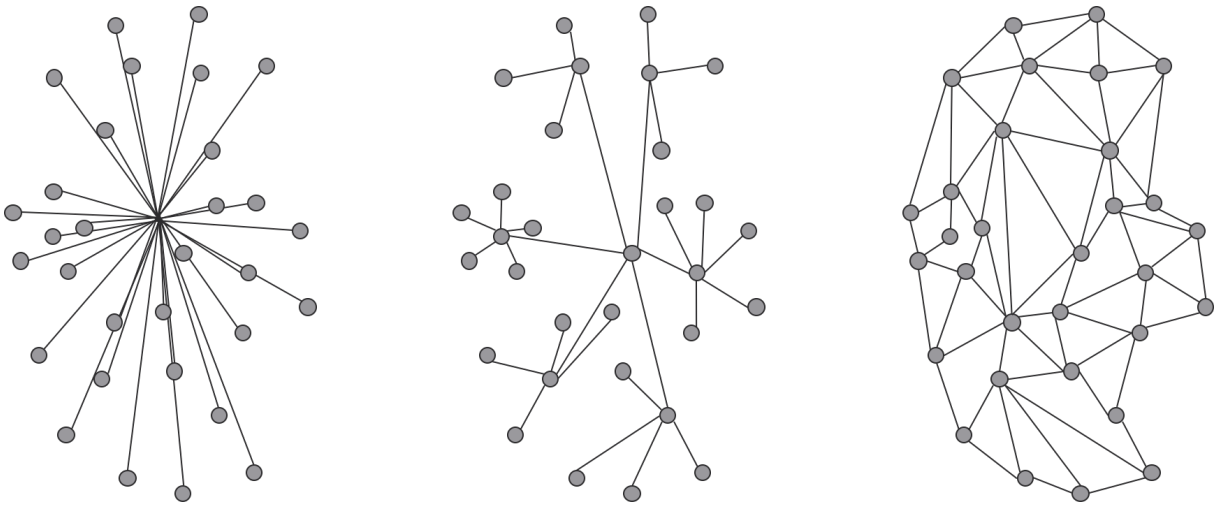

FIGURE 2: CENTRALIZED, DECENTRALIZED, DISTRIBUTED STRUCTURE

Furthermore, each node, regardless of its level, can play two roles within the network:

- "**Miner node**" (term derived from the Bitcoin protocol): these nodes directly support the operation of the blockchain by carrying out operations of verification and

confirmation of transactions and the drawing up of the register itself (as this will happen later)

- "**Wallet node**": these nodes manage a series of addresses that identify the node and the user. This list allows to send and receive transactions with respect to the other users

Roles and levels combine to create four types of nodes [8]:

1. Light, wallet node: generally represented by mobile users, it allows to carry out transactions but not to participate directly in the operation of the network
2. Light, miner node: given the profitability of the mining activity, many clients gather in what are called "pools" of users, where they participate in the creation of the ledger, sharing the revenues and sharing the workload
3. Full, wallet node: they are desktop users and service providers that focus only on the management of transactions without carrying out mining operations
4. Full, miner nodes: they are divided into pool servers, which manage and organize pool clients, and mining farms which instead specialize in mining and acquire significant computing power.

Thus, each wallet node transmits to the network the transaction a user wants to make, this happens in broadcast mode which means that this transaction is communicated to all other nodes in the network. At this point each node that listens to the transaction, after a check of formal correctness and status of the user, begins to build a block. A block is nothing more than an aggregate of operations, which must meet some of the requirements of the confirmation algorithm. Once the block is complete, it is proposed by the node to the network, and, simultaneously, all nodes communicate their version of the block. Through a consensus algorithm a majority agreement is reached on which block to insert and add at the end of the blockchain. Later on, the confirmation requirements necessary to transmit the block will be explained, while now it is important to note that changing a block means having to change all the subsequent ones and then the whole chain following the counterfeit node must be reworked so that each block meets the necessary confirmation requirements.

A consent algorithm allows you to create what is called a *trustless trust* between the nodes. In other words, this defines how to make credible the proposal of a block to be added to the blockchain and how to converge to a shared version of the ledger.

The literature poses this problem of trust between the nodes of a network as the "problem of the Byzantine generals" [9] which is already described in the introduction of this paper. Analyzing deeply the problem, the complication lies in the fact that some generals may be traitors and push some generals to attack and others to flee, so as to cause a defeat and huge losses for the army; moreover, the communications are made through a corruptible messenger. The problem can only be solved if the traitor generals are in a minority compared to the loyal ones. This remains valid even for a blockchain, so the model will have to make terribly difficult the concentration of mining activity at some nodes that could be malicious.

The different protocols have presented various consensus algorithms, the main ones of which are presented below, in order of degree of decentralization (from the most decentralized and least efficient to the least decentralized and most efficient):

- **Proof of work:** The network takes into consideration only the blocks proposed by those nodes that demonstrate to have dedicated a certain amount of work to the drafting of such, for example solving a complicated mathematical puzzle. This puzzle must be constructed in such a way that it is expensive to find a correct solution to the problem, but at the same time it must be quick to verify the correctness of such a solution [3]. It is therefore said that the probability of opening a new block of a node is directly proportional to its computing power
- **Proof of capacity and proof of storage:** Similar to proof of work algorithms, this method also involves exploiting the hardware capabilities of the node. However, these algorithms use memory, not computing power, resulting in more energy-efficient algorithms [10]
- **Proof of burn:** The idea behind this method is that to undermine a node needs to burn currency. In practice, to be able to write on the node you have to send a certain value to blocked addresses. This is expensive from the point of view of the node in economic

terms, but not from the point of view of energy and time. In contrast to this, current proof of burn technologies requires that a currency previously undermined by proof of work has to be burned, thus these current technologies only move the problem without resolving it [11]

- **Proof of elapsed time:** This algorithm provides that each time a new block is added, each node waits for a random number of seconds and that the one waiting for the lowest number of seconds is the one that actually adds the block to the chain and is then rewarded. The guarantee that the nodes respect the rules derives from the characteristics of the environment in which these algorithms are executed; this is possible for example by using the Intel Software Guard Extension (SGX), an extension that, combined with specific hardware, creates certificates that guarantee that a certain code is actually running in that environment [12]
- **Proof of stake**: In this case we don't take into account the computational capacity dedicated to the solution of a problem, but other parameters such as the amount of crypto currency owned by the node itself. In practice, if a node has 10% of all the tokens of that blockchain, then it will have a chance to write the new block equal to 10%. In theory, this system should discourage nodes from creating a deviation of the block chain (falsifying a node), since if his deviation were not the one which would win, he would have lost time and therefore relative power in the network [13]. Actually, ironically, what happens is that, while for bitcoins this is expensive, in case of proof of stake algorithms, it costs nothing to try to carry out dishonest actions [14]
- **Reputation based:** these consensus algorithms give priority to some nodes considered more authoritative based on the number and intensity of the interactions between them and the other nodes (the most active nodes) [18]
- **Proof of authority:** This algorithm is a modified form of proof of stake algorithms where "stake" is no longer monetary value but the identity of the node, in this way only nodes whose authenticity is verified can participate in the writing of the register. This algorithm is typical of private networks, as nodes are not anonymous and must be allowed to write on the register [19].

From a historical context point of view, the Bitcoin protocol uses a proof of work algorithm, while the currencies created later, such as Ethereum and Ripple, are moving towards increasingly efficient, but less decentralized, models.

Furthermore, it is important to remember that there is a reward for the nodes that participate in the writing of the new blocks. This was established to promote the sustenance of the network (to push the nodes to participate in the writing phase) and to make the attempt to counterfeit a block economically unattractive [22].

2.1.2 DLT FUNCTIONING

To conclude the speech on how distribute ledger technologies work, more commonly called blockchains, will be explained, more specifically, their operation and the different types of networks and blockchain. In this paragraph the operations and the practical functioning of a transaction through blockchain will be explained.

Since the scope of this work is to analyze and compare the classical way to raise capital (IPO) and a new one (through security token), it was decided to propose as an example some extracts of the Ethereum (which is more appropriate for the thesis purpose) white paper (protocol) [25] to better understand how some of the concepts mentioned so far are put into practice. To understand better the Ethereum functioning and its application to the capital market world, it was decided to propose in the first place, as a preparatory example, some extracts of the Bitcoin protocol [3].

Bitcoin

As mentioned above, in order to exchange money, users must have addresses at their disposal that are equivalent to the IBAN code of bank transactions. Generally, blockchains, and Bitcoin is not an exception, allow to generate new addresses for each transaction, ensuring a strong anonymity to users. For the purpose of this document it is sufficient to explain that the address

of the user of the Bitcoin network derives from his public key (that of the digital signature) and that in this way it is guaranteed that the user is actually associated with the address. In other words, the address is a shorter and more readable version of a public key and guarantees the user address correspondence by exploiting the mechanism of the digital signature.

Each node that carries out a transaction communicates it to all the other nodes in the network and these add it to the write block. To encourage the nodes to include the transaction in the block, a reward is provided for those nodes that include it in the block that are undermining; generally, the value of the reward is decided by the user or by the wallet. In addition to this, there is also a "new" bitcoin reward, which is generated together with the block and assigned to the node that first completes the block. For this reason, the process of writing blocks is called mining.

The Bitcoin protocol uses a proof of work consensus algorithm. When a miner node receives enough transactions, it creates the block to add to the chain, including the digest (or hash[4])

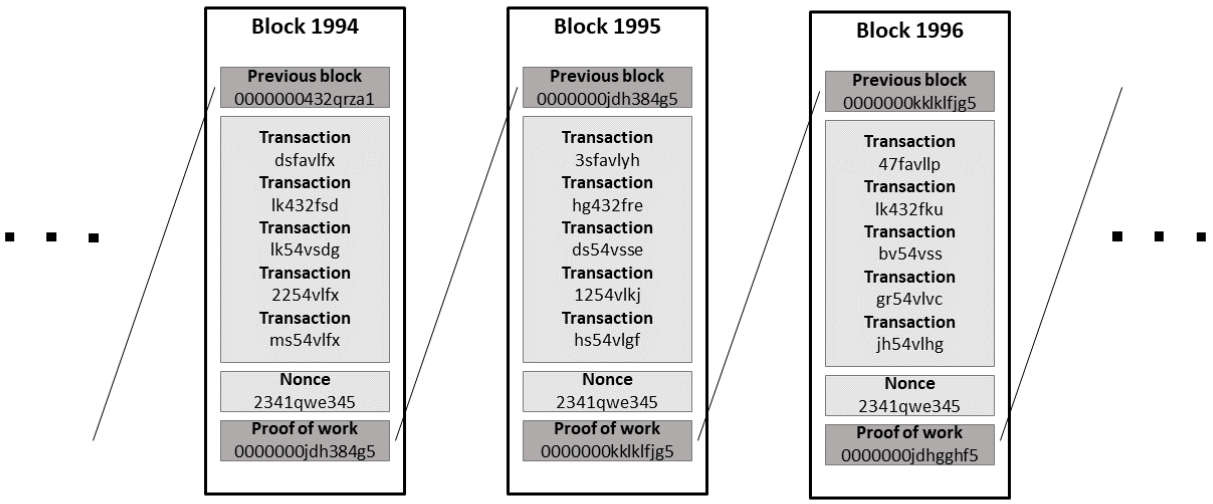

FIGURE 3: BITCOIN BLOCKCHAIN SIMPLIFIED STRUCTURE

[4] A hash is a string of values created from a string of text using a mathematical function. (Cryptography elements are not explained since are not necessary for the purpose of this thesis).

value of the previous block as the first value, so as to connect it to the current chain (Figure 3).

The proof of work provides a puzzle structured as follows: the miner must add as the last value of the block a number called "nonce" that must cause the hash function applied to the whole block (containing this number at the end) to start with 30 zeros. The chances are that this will happen about one in a billion and since there is no way to start from a hash and find the message that generated it, each miner must try all possible numbers until he finds what gives the desired result. Also, thanks to the properties of the hash function, once you have a block with corresponding nonce, it is immediate to check that this gives a hash that starts with 30 zeros. Once compiled like this, the block is sent to all the other nodes on the network, which check that the nonce is correct and add it to their blockchain (to their ledger).

Now it’s presented the case of a dishonest knot. In this situation the dishonest node will create a block with one or more falsified transactions, which therefore the other nodes, involved in writing the block, do not know.

It may happen that this node is faster than all the nodes and can solve the puzzle first and then send the fake block to the whole network. The knots will be assumed to believe that the nde is correct, but after a while also the blocks by the other mining nodes blocks will be communicated. An honest node will then receive two blocks that compete for that position, one correct and one false. The honest node then creates a bifurcation of the chain (Figure 4), one for each of the two blocks; at the end the node chooses and takes as true the longest one, that is the one where blocks arrive faster from the other nodes; given the amount of work needed to continue to write blocks, it is much more believable a chain composed of several blocks. In practice, the dishonest node that solves the puzzle before the honest nodes must continue its chain to give credibility to that node. In fact, being each block connected to the previous one through its digest, changing a block at some point in the chain means to modify all the following ones too. Therefore, as far as it is possible that a node falsifies a block in time, it is rather unlikely that it will be able to continue to compile blocks of its "falsified chain"

faster than all the other nodes in the network. The number of successive blocks used to validate a block with a high level of trust is about 6 [23].

Finally, it should be noted that in this protocol it's used a hash function starting with 30 zeros and that this number is automatically changed by the protocol so that the resolution time based on current technology is about 10 minutes. Moreover, the compensation given to the miner who first creates the new block is regulated by an algorithm that halves the value of the prize every 4 years, in a geometric way so that the maximum number of bitcoins in circulation is limited; for this reason a payment in percentage is also foreseen for the process of inscription of a block.

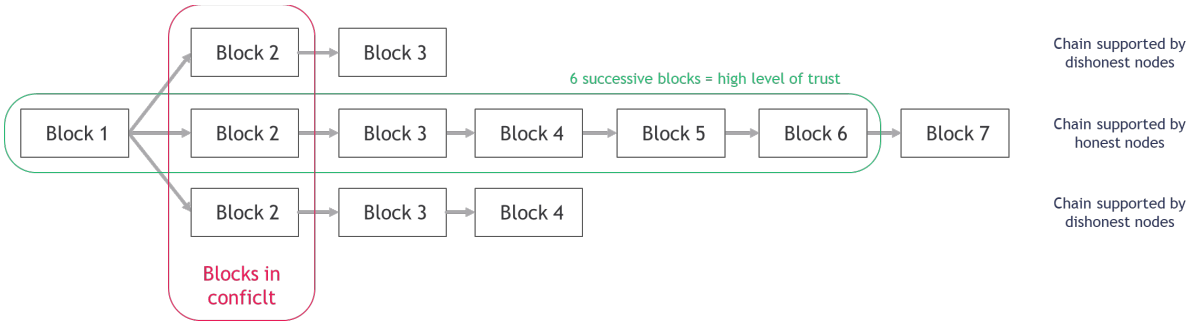

FIGURE 4: CONFLICT MANAGEMENT IN THE BITCOIN PROTOCOL

Ethereum

Ethereum blockchain is quite different from the previous one since its scope is "to allow developers to create arbitrary consensus-based applications that have the scalability, standardization, feature-completeness, ease of development and interoperability offered by these different paradigms all at the same time." (Vitalik Buterin, 2013) There are some new elements and differences that have to be introduced to properly explain Ethereum functioning:

- **Ether:** each activity on Ethereum that change its state costs Ether which is the currency of Ethereum and it's used as fee. Miners who successfully generate and write a block in the chain are rewarded with Ether. Ether can be converted into traditional currencies through the classic Crypto-exchanges. Ethereum uses a metric system of denominations used as units of ether. The smallest one, which represents the ether base unit is the Wei. In the figure below (figure 5) all the denominations are represented from the smallest, the Wei, to the biggest one, the Tether.

```
'wei':          '1',
'kwei':         '1000',
'ada':          '1000',
'femtoether':   '1000',
'mwei':         '1000000',
'babbage':      '1000000',
'picoether':    '1000000',
'gwei':         '1000000000',
'shannon':      '1000000000',
'nanoether':    '1000000000',
'nano':         '1000000000',
'szabo':        '1000000000000',
'microether':   '1000000000000',
'micro':        '1000000000000',
'finney':       '1000000000000000',
'milliether':    '1000000000000000',
'milli':         '1000000000000000',
'ether':        '1000000000000000000',
'kether':       '1000000000000000000000',
'grand':        '1000000000000000000000',
'einstein':     '1000000000000000000000',
'mether':       '1000000000000000000000000',
'gether':       '1000000000000000000000000000',
'tether':       '1000000000000000000000000000000'
```

FIGURE 5: ETHER METRIC SYSTEM

- **Gas:** since, as it was just explained, Ether is traded on Crypto-exchanges, its price is not fixed and depends on the Crypto-exchanges demands and offerings. This implicate that the price of using a service in Ethereum could be different day by day since the Ether used to pay fees will have a daily different price. For tis reason, there is the serious risk that people will wait for a low price of Ether to execute their transactions and, obviously, this is not is not the ideal situation for a platform like Ethereum. Gas represents a solution to this problem. Gas is the internal currency of Ethereum and the execution and utilization cost of the Ethereum services is predetermined in terms of Gas units (Gas cost). The Gas price is adjusted to balance the fluctuating cost of ether. For example, to invoke a function in a contract that modifies a string will cost Gas which is pre-determined, and Users should pay in terms of Gas to ensure smooth execution of this transaction. [26]
- **Ethereum Virtual Machines nodes (EVM) vs Mining nodes:** in Ethereum, contrarily to the Bitcoin, the blockchain network consists of multiple nodes which belong to miners

and other nodes that help in execution of smart contracts and transactions but they do not mine. These nodes are the EVM. Each node is connected to other nodes on the network. These nodes use peer-to-peer protocol to talk to each other. The EVM can access accounts, contract and externally owned, its own storage data but it does not have access to ledger. It has limited information about current transaction. EVM are the execution component in Ethereum and its scope is to execute the code in smart contract line by line. However, when a transaction is submitted, the transaction is not executed immediately instead is it pooled in a transaction pool. Thus, these transactions are not yet executed and not yet written to the Ethereum ledger. EVM nodes are similar to mining nodes however they do not do mining. The miner nodes have to write the transaction on the chain. They are interested in doing that because of the reward they will receive, similarly to the Bitcoin blockchain. There are two types of reward: thereward for writing a block and the cumulative gas fees from all transactions in the block. As for the Bitcoin blockchain, the miners try to solve the puzzle using its compute power and the first which manages to do it receive a reward of 5 ether. Each miner node maintain its own instance of the blockchain ledger which is the same for all the miners. These nodes are part of the same network where EVM is hosted. At a certain point of time, the miners would create a new Block, collect all transaction from transaction pool and adds them to the newly created block. Finally, this Block is added to the chain. [26]

- **Proof of work vs proof of stake:** is the same already explained consensus algorithm already explained for the Bitcoin blockchain. Proof of stake is the consensus algorithm which will be used in the latest Ethereum protocol[5]. "Generally, a proof of stake algorithm looks as follows: the blockchain keeps track of a set of validators, and anyone who holds the blockchain's base cryptocurrency (in Ethereum's case, ether) can become a validator by sending a special type of transaction that locks up their ether into a deposit. The process of creating and agreeing to new blocks is then done through a consensus algorithm that all current validators can participate in. There are many

[5] Ethereum 2.0 is an upcoming update of the Ethereum network, which aims to improve the level of security, scalability and decentralization of the blockchain.

kinds of consensus algorithms, and many ways to assign rewards to validators who participate in the consensus algorithm, so there are many "flavors" of proof of stake. From an algorithmic perspective, there are two major types: chain-based proof of stake and BFT-style proof of stake. In chain-based proof of stake, the algorithm pseudo-randomly selects a validator during each time slot (e.g. every period of 10 seconds might be a time slot), and assigns that validator the right to create a single block, and this block must point to some previous block (normally the block at the end of the previously longest chain), and so over time most blocks converge into a single constantly growing chain. In BFT-style proof of stake, validators are randomly assigned the right to propose blocks, but agreeing on which block is canonical is done through a multi-round process where every validator sends a "vote" for some specific block during each round, and at the end of the process all (honest and online) validators permanently agree on whether or not any given block is part of the chain. Note that blocks may still be chained together; the key difference is that consensus on a block can come within one block, and does not depend on the length or size of the chain after it." (Vitalik Buterin, 2019) [25]

- **Esternal owned accounts vs Contract accounts:** external woned accounts are the ones owned by people. In Ethereum these accounts are not referred by names, hence when one of these accounts is created on Ethereum, apublic-private key of 256 characters (even if only the first 160 are used to represent the identity of an account) is generated. The individual keeps safe his personal key while the public key becomes the identity of this externally owned account. An externally owned account can hold Ether, or other crypto-currencies based on ether, in its balance and do not have any code associated with them. These accounts work like bank accounts: they can execute transactions with other externally owned accounts and they can also execute transactions by invoking functions within contracts. Contracts accounts are very similar to externally owned accounts. They are identified using their public address. They do not have any private key. They can hold ether similar to externally owned accounts even if they just contain code for smart contracts consisting of functions are state variables.

- **Transaction:** Ethereum basically helps in executing transactions of three types: 1) transafer of ether from an account to another (externally owned or contract accounts); 2) Smart contract deployment done by an externally owned account using a transaction in EVM; 3) Executing a function in a contract that changes state are considered as transactions in Ethereum (If executing a function does not change state, it does not require a transaction). There are some important properties which define each transactions and are related to it (From, To, Value, Input, Blockhash, BlockNumber, Gas, GasPrice, Hash, Nonce, TransactionIndex, Value, V, R and S).
- **Messages:** “"Messages” in Ethereum are somewhat similar to “transactions” in Bitcoin, but with three important differences. First, an Ethereum message can be created either by an external entity or a contract, whereas a Bitcoin transaction can only be created externally. Second, there is an explicit option for Ethereum messages to contain data. Finally, the recipient of an Ethereum message, if it is a contract account, has the option to return a response; this means that Ethereum messages also encompass the concept of functions.” (Vitalik Buterin, 2013).
- **Blocks:** contains transactions. A single one contains multiple transactions and each block has a different number of transaction based on Gas. Each block has an upper Gas limit and each transaction needs certain amount of Gas to be consumed as part of its execution. The cumulative gas from all transactions that are not yet written in ledger cannot surpass the Block Gas limit. This ensures that all transactions do not get stored within a single Block. As soon as the Gas limit is reached, other transaction is removed from block and mining begins thereafter. Blocks form the blockchain and, as for the Bitcoin, they have a parent-child relationship but the first one, the genesis block.
- **Smart contracts:** A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible (Wikipedia, 2019). Fundamentally, a smart contract is a contract implemented and executed within Ethereum ecosystem. It can be considered as a kind of digitization of a legal contract. They are deployed, stored and executed within EVM and can store data. The data stored can be used to record

information, fact, associations, balances and any other information needed to implement logic for real world contracts. Moreover, they are very similar to object oriented classes since they can call another smart contract to create and use objects of another smart contract.

Back to the transaction example presented in the Bitcoin example, here below (Figure 6) is presented how a transaction would be on the Ethereum blockchain.

Let's suppose that Vittorio wants to send money to Marco. Vittorio generates a transaction message containing From, To, Value fields and sends it across the network. The transaction is then placed in the transaction pool as is previously explained. A miner node (it's the same for all miners on the network) creates a new block and takes the transactions from the transaction pool (taking in account the Gas limit criteria) and adds them to the block (including Vittorio's one). Following the consensus logic used in the protocol, the miners validate and verify the block and consequentially accept the new block, which contains Vittorio's transaction, and adds it in their ledger. Therefore, a new block that is persisted across time and space is created and added on the chain. During this time the accounts of both the parties are updated with new balance. Finally, the Block is replicate across every node in the network.

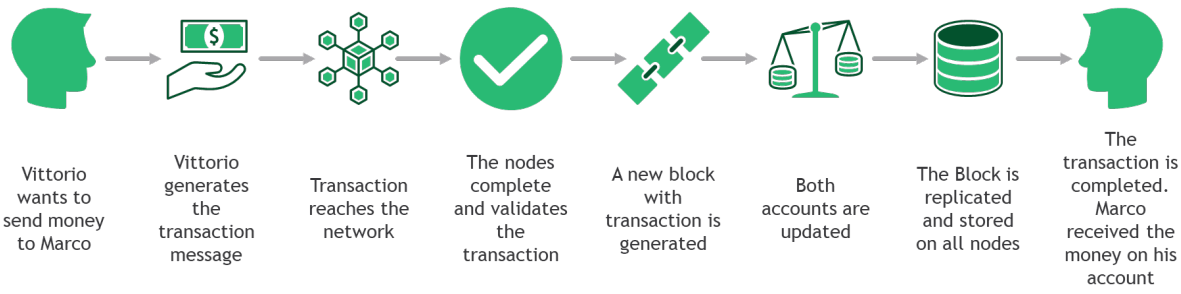

FIGURE 6: TRANSACTION ON THE ETHEREUM BLOCKCHAIN

The particularity of Ethereum is that, thanks to the Smart Contracts and its architecture, it has a wide range of applications. The primary difference between Ethereum and any other cryptocurrency is that it is, as explained above, an environment and not just a currency. On Ethereum, everyone can build their own projects and DApps (decentralized applications) through smart contracts. This shows the true scope of what is possible in Ethereum. As

identified, by Buterin, in the Ethereum white paper, this technology fits very well three types of applications:

1. Financial applications, providing users with more powerful ways of managing and entering into contracts using their money. This includes sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and ultimately even some classes of full-scale employment contracts [25].
2. Semi-financial applications, where money is involved but there is also a heavy non-monetary side to what is being done; a perfect example is self-enforcing bounties for solutions to computational problems [25].
3. Applications such as online voting and decentralized governance that are not financial at all [25].

For the purpose of this thesis, it's necessary to focus and explain better how a token system works and why this technology can be used to revolutionize the capital market world.

On-blockchain token systems have many applications ranging from sub-currencies representing assets in the real world (EUR, silver, company stocks, etc.) to individual tokens representing smart property, secure unforgeable coupons, and even token systems with no relationship to conventional value at all. Ethereum seems to be the perfect environment in which to implement these token systems. A token system basically is a database with one operation: subtract X units from A and give X units to B, with the proviso that (i) X had at least X units before the transaction and (ii) the transaction is approved by A. Thus, to implement a token system we just need to implement this logic into a contract.

Smart Contract: in-depth analysis

In this section it has been chosen to present an in-depth analysis of smart contracts given the centrality of their use in security tokens.

As already said, smart contracts are pieces of code that run on a blockchain that contains a set of rules under which the parties to the contract have agreed to comply. When the conditions of these rules are respected by the system, what is agreed in the contract is automatically

executed. These tools facilitate, verify and apply the negotiation between two or more parties, redistributing the assets that they bring into play. As the name suggests, they are contracts that do not need any central authority to monitor their compliance and implementation, although they are not yet a legal instrument [24].

The term smart contract was born in 1996, years before Bitcoin, as an alternative to traditional legal contracts that are often accompanied by high costs of agreement and enforcement. The smart contract was born only to reduce costs and time, automating the contract process, but it is only with the arrival of the blockchain that the idea was supported by a technology which is able to fully do that. In fact, the blockchain allows anyone to enter code in the network in an indelible and guaranteed way, without the possibility of counterfeiting.

The technical functioning of a smart contract and of the Ethereum blockchain was showed in the previous paragraphs.

Smart contracts could be the tool to digitize most of the legal obligations, thus reducing the burden on the institutions, however several problems still persist [27]. First of all, as a code it depends on the developers themselves who may not take into account some aspects and thus undermine the bond at the beginning (as happens with lawyers and regular contracts). In the same vein, it should be pointed out that in terms of information security, these tools still require many studies, since at the moment their vulnerabilities are not fully known [28]. Secondly, often these contracts have constraints that formalize events that occur outside the network itself, it is therefore necessary that there is a transitional element between the blockchain and the outside world, this is called "oracle" or "gateway". These oracles collect information from the outside world (think of a person who enters data or a bot who collects it on the web) and write it on the blockchain, based on this new information, smart contracts then perform their operations. Of course, it is also possible to make the oracles work in reverse, that is, in such a way that they communicate to the outside world what has happened on the net. These elements of conjunction represent, however, a point of failure that becomes of fundamental importance for the success of the entire process [29]. Thinking about the role

of the oracle, it immediately comes to mind that it is not yet possible to translate all the physical actions of the real world into code or vice versa.

To better appreciate what these tools can offer, the example of the sale of a car between two individuals is presented below. Traditionally this process involves some bodies that verify and certify the transfer of ownership and the transfer of money between the two parties. In a more technologically advanced scenario, on the other hand, it can be expected that something much more automatic will happen without the intervention of other bodies. The seller fills in the smart contract with the price and ID of the car in question, and the buyer signs it confirming that he is willing to pay that amount. The blockchain now checks on the one hand that the ID corresponds to something actually owned by the buyer (represented by one of the tokens associated with him) and on the other hand that the balance of the second individual is sufficient to cover the amount; if these conditions are met then the network transfers the token representing the car to the buyer and the amount to the seller. If the car is then supposed to be opened and started with a completely digital block, the blockchain associates the digital signature of the new owner to the car and in so doing the process is fully automated. The sale of the car is completed without any intermediary party.

2.1.3 PUBLIC AND PRIVATE NETWORKS

The different protocols that have been developed in recent years have sometimes restricted the freedoms granted by the Bitcoin protocol to users: both from the point of view of anonymity and from that of trust. In fact, on these two levels, different categories of blockchain have been created: there are some networks in which only some users (therefore identified) have access, called private networks; and some other networks in which only some nodes can participate in the writing of the register that, given the need for this permission, which are called permissioned [24]. Although no formal agreement has yet been reached on how to classify blockchains in these terms, the solution that seems to be spreading more and more is the following [25]:

- **Public blockchains**: these are blockchains as proposed by the Bitcoin and Ethereum protocols, in which anyone can participate, both in reading and in writing the register. These are protocols that do not require any kind of trust between the nodes, and that guarantee the consistency of the register thanks to the goodness of the protocol itself.
- **Blockchain public permissioned**: in this case any user can access the blockchain and carry out transactions, however only a limited number of nodes can participate in the consent algorithm and thus the writing of the register. For example, altcoins like Ripple are part of this category.
- **Blockchain private permissioned**: in the latter case, users who want to be part of the network must also identify themselves and be authorized by another entity before having access to the blockchain. In addition, the process of writing the ledger is generally entrusted to some trusted central authorities. Blockchains of this type require that users belong to the same entity, such as a company or a consortium of such users.

As well as the different consensus algorithms, the types of blockchain listed above weigh differently some values of technology, such as anonymity and equality between nodes. Starting from public and moving to private blockchains, we lose anonymity, equality, decentralization (the disruptive elements of technology) in favor of greater efficiency in terms of computing and therefore cost. Moreover, although in a permission-less blockchain there is no economic convenience in the collusive behavior between the nodes (due to the possibility of entering the network for free), this is not true in a permissioned context, where instead the closure of the network allows the nodes to find a balance in the collusion [7]. It is therefore clear that this last type of network is seen as a solution that offers lower computational costs and higher number of transactions performed compared to the original blockchain, sacrificing its decentralized aspect.

2.1.4 TYPES OF BLOCKCHAIN

There is not yet an exhaustive and precise classification that allows to analyze with care the various blockchain protocols, but they have been born from different points of view and different frameworks. Some classify the blockchain according to the type of visibility that is given (public or private) or according to the consent algorithm adopted, as seen above.

By tackling the issue with a view to increasing abstraction and from a functional point of view, it was decided to divide, in this paper, the blockchain technologies according to the level at which they operate, whether it is that of the blockchain itself, smart contract, or even decentralized application. In fact, a decentralized application uses smart contracts to put users in contact, passing through a blockchain.

The solution that is deeply analyzed here is, instead, based on the implementation type and comes into contact with some technical aspects of the protocols that allows the reader to better appreciate how this technology can exploited. The classification is proposed by the European Banking Authority and therefore comes from a point of view that takes into account mainly the examples that directly affect the banking sector, while applications are now ranging to all industrial sectors. With this in mind, the proposed categories of blockchains are as follows [26]:

- Digital currencies.
- Asset registry
- Application stack
- Asset centric technologies

Digital currencies

The technology used in this category aims to create crypto-currencies of various kinds, the purpose of which is precisely to offer an alternative payment service to the traditional one. At the level of possible application there is an analogy with what is already offered by legal

tender, therefore from speculation to payment, without an institutional context. Examples of this category include Bitcoin, Litecoin, Peercoin, Dogecoin and currently thousands of other currencies that represent the historical and main application of this new technology born with the Bitcoin protocol. The cryptocurrencies are based on a reliable register shared between nodes of the same level (and not entrusted to a single one), transactions protected and verified through cryptographic techniques, and consensus algorithms.

Asset registry

These "asset registers" use distributed registers to record transactions of other assets, not just money. To do so, they include in a transaction of little value a link to an external asset, whose transaction is thus imprinted in the blockchain and the ownership follows the token on which it is registered. It is as if they were creating a second register within the main register, thus exploiting its portability and security. Examples are Mastercoin, Coloredcoin and Namecoin. The main technique used is the writing of metadata (data not essential to the transfer of currency) in the various transactions and for this reason they are called "Metacoin". Obviously this process “get the blockchain dirty”, as it pollutes its data, increasing the size and time of the register, creating the problem that is called "blockchain bloat". This problem then adds to the different obstacles to the scalability of the blockchain.

Application stack

In this category we find applications that move to a higher level of abstraction, thus shifting the focus of the search towards blockchain that no longer only offer a currency. In other words, they offer a blockchain on which to develop applications that exploit the underlying blockchain as a single carrier technology, without affecting it or worrying about its operation. For example, we propose Ethereum, Next and Eris. The main purpose of these blockchains is to become a platform for the development and execution of fully decentralized applications, similar to the various cloud services of Microsoft and Amazon. Decentralized applications are smart contracts, Decentralized Applications (DApps) and Distributed Autonomos Organization (DAOs). These are considered as front-end applications equal to the traditional ones, but supported by a blockchain rather than by a client server architecture.

Asset centric technologies

This category includes technologies such as Ripple, Stellar and Hyperledger that focus on exchanging digital assets in combination with a shared, but not publicly available, ledger. Trust between nodes is created directly between participants and not through a Bitcoin-style blockchain. The protocol acts as a router between the various nodes and allows, moving only between nodes where there is a relationship of trust, to put nodes in contact between which this relationship does not exist. In this case the protocol does not provide that each node saves all the transitions, but only a part. In this way the transactions are recorded through a consensus algorithm in an almost instantaneous way. Generally, the participants in these networks are entities that already have trusted relationships outside the network, in the physical world, and use this mechanism to automate the exchange process by reducing time and cost, in a system that is still verified and secure, such as the blockchain. The main feature of these systems is that the parties involved can exchange various types of assets, even non-digital, which do not have to be native to the application, unlike what happens in classic blockchain such as bitcoins. Obviously, moving from the physical asset to the digital one, we are faced with the problem of how to ensure security and confidence in the gateway that acts as a bridge between these two worlds. In a context like this of institutional trust it is not a problem.

The classification just seen is perfect to highlight the possible applications of technology.

2.2 SECURITY TOKENS

This section will explain the definition of security tokens, the definition of security and all the concepts necessary to fully understand the functioning of this particular application of DLT technologies to the asset market in general. As there is not yet an adequate and complete literature dealing with the subject, it would be good to be able to consult the opinion of the experts and of the direct participants in the development of these technologies. Fortunately,

a precious podcast "Flippening - For Crypto Investors" [61 - 62 -63], conducted by Clay Collins, CEO of Nomics (a crypto-data firm), has allowed to collect different information and the opinion of some of the most involved, famous and prestigious actors in this field.

It is important to note that, since most of the speakers and major players are in the US or refer to the US market, the following paragraphs will almost always refer to the processes and laws used in the US. Later on (in section 2.3.3 of this thesis) a vision of what has been said for European processes and laws will be presented.

2.2.1 INTRODUCTION TO SECURITY TOKENS

There are three main misconceptions about security tokens that will be faced during the following lines and that will be shoot down. The three misconceptions are:

1. The first misconception is that security tokens are not valuable, because they are centralized around the issuer and in many cases are not censorship resistant.
2. The second misconception is that securities should not be represented with a blockchain because securities are not, at their core, digital assets.
3. And the third is that security tokens are overkill and that all that is needed is a highly efficient database, rather than a blockchain, to address the needs of issuers and traders. [35]

To fully understand the security token concept, we should start addressing two questions: what is considered as a security? And how did the security system work? What can be improved?

In US a security is defined by the Howey Test which can be seen as a set of conditions used to determine what is and what is not a security. It is a four-part test which qualified something as a security if it involves: 1) an investment of money 2) in a common enterprise, 3) with the expectation of profit, 4) deriving predominantly from the efforts of others. But, as emerged

from the experts' opinion, the fourth part is the most important one. Thus, if, for example, you have a fractional ownership of a Picasso artwork, and it value and price depends only, as it is today, on the demand and supply laws, it would be not a security. While if you invest in company shares or in other securities themselves, those would be securities even if you do it through tokens as it is explained later.

So, now that the definition of security is clear, let's address the next question: what is a security token? Security tokens are, in practice, the same security interests which exist today, only with electronic wrapper. A great analogy could be to compare email to snail mail and the evolution of the writing messages' process. Typing out the same exact written communication, 25 years ago, the process would require to click Print, then to put it in an envelope, put a stamp on it, wait and have it delivered after few days. Nowadays, all the process could be done by just clicking Send on an email and it happens instantaneously at almost no cost. The content of the written message would be exactly the same, whether it's in electronic medium or paper medium, but the real difference is that once something is electronic and digital, it can be sent faster, cheaper, and easier by orders of magnitude. Similarly, with photography, whether a film or digital sensor is used, the photo of the object looks the same. The main difference, again, is that digital photography is orders of magnitude, faster, cheaper, and easier to develop or use the images. In a similar way, when a security is tokenized or digitized, it can be issued or traded, orders of magnitude, faster, cheaper, and easier. Obviously, this transformation leads to transformative uses that were not knew before.

In the next section (2.2.2) the actual functioning and application of the security tokens will be explained. In this section the focus on its potential functioning is maintained. There are several aspects of the actual application of DLT technologies to the trading and issuing of capital, which could be interesting for the purpose of this thesis. It was choosen to distinguish two different applications of security tokens: to private and to public companies.

The private security market, today, exists only on paper and have zero liquidity. Given the absence of technologies and the presence of many restrictions (mainly due to the lack of controllability and security of the process) today the issuing and trading of the shares tested

requires a lot of time and a high price. Today, in the US, there are special restrictions on the affiliates of the issuer of shares, so not only to subsidiaries, but also to persons who have a controlling interest or controlling influence in the issuer. There are a number of issues that the issuer must control. The way they do it today with private securities, which exist in paper, is that they put these strict transfer restrictions on which you are obliged to go to the issuer and manually obtain a waiver in case you want to sell your shares. Then you need to go and look for the counterparts to buy your shares. Assuming there were 50 or 100 interested investors, there would be many fax, phone, or email numbers, and the whole process would take a long time to find someone. As a result, when you have a private investment and you need liquidity it takes weeks or months. It takes a lot of work, there are major costs (like $10,000 per rep per transaction) and then there is what is called illiquidity discount. This is always applied to the transaction that suffers a major blow on its valuation. Academic literature says that this discount amounts to 20-30% of the entire value but, in fact, if you want to speed up the process, it can be deeper than that. Security tokens brings two main advantages to this system. The first one is that the entire system will become more technological, thus easier to use and control and cheap. The new technology could do it taking some of these costs that are involved in transaction and automating them to some extent, which makes it easier to transfer these assets, and reduces the direct transactional costs relative to moving value. The implicit second advantage is the most transformative one: the solution for the illiquidity premium. In fact, using security tokens, an exchange of tokens would be available to every investors. Furthermore, the market depth of the private company shares will be amplified. The combination of those two reasons will automatically bring liquidity to the assets. Finally, thanks to the previously explained functioning of DLTs, it would be always possible to have an up-to-date and verified cap table. This aspects increases a lot the cap table management system of the private sector companies.

Obviously all the advantages just discussed, regarding the liquidity, are easily applicable and transferable to the secondary market.

The advantages for the public securities markets would include some administrative efficiencies using blockchain technology such as: faster and easier settlements or more

accurate cap table management, but for public securities today, shares in a public company, tokenization doesn't offer a real transformative value [35]. The issue here is mainly limited to the technical aspects of the securities issuing and trading processes. However, we must be careful to specify that when we speak of exchange, we are not talking about what is commonly called trading, but of effective exchange of ownership from one owner to another. In fact the digitized system currently used in Wall Street and all over the world to make trading works very well and with very short times that allow you to make multiple transactions in a practically instantaneous way. It must be specified however that every time that someone exchanges, buys, sells a Stock, through a platform of trading, does not happen an effective exchange of instantaneous Stock between the brokers that hold the Stock of the investors. The exchange takes place only at the end of a certain period (day), net of all the exchanges made. These would be off-chain transactions, made at the end of the day. The security token revolution does not change the high-frequency trading, but it will make the real money transaction at the end of trades easier. Also, on the investor side, it will give people more control of their own money because they will be more liquid and easier to track and manage. As already mentioned, one of the real advantages for public companies will be the management of their "cap table" or, to be more precise, of their shares issued on the market. Today, given the presence of various parts that manage the shares, and the various layers of the system of holding them (through banks, brokers, other financial institutions) it is almost impossible for a listed company to have a clear, safe and immediate idea of who holds its shares issued on the market at all times. Clearly, the support of DLT technology would make everything instantly traceable and secure and would allow better management and control of their shares on the market [35].

To conclude this part, there is an opinion shared by most experts, who suggest that the best way to make the regulation environment agree with the DLT is not to create a new regulation around it but to make the current regulatory system less cumbersome to comply with tokens.

Here below a small recap of the potential advantages which may occur in case of the adoption of the security tokens. They:

- increase liquidity and market depth;
- give control back to security owners;
- increase the number of liquidity options for security owners such as peer-to-peer exchange and decentralized exchanges;
- maintain the cap table for private companies (= easy cap table management);
- provide cap table analytics to public companies (= public companies would actually see who owns their shares);
- allow for fractional ownership of property like paintings;
- reduce settlement times from two days to minutes;
- make it cheaper to go public.

2.2.2 How security token platforms work

A streaming video, which aired in April 2018 on Periscope, has become very popular among members of the blockchain community. The video was shot by Bruce Fenton[6], popular in the community and owner of Atlantic Financial, a full-service investment firms. The video immediately became viral as Bruce was actually tokenizing ownership of his company, Atlantic Financial, and he did it in more or less ten minutes using a web browser, a piece of paper, and ten dollars. This streaming video proved to all intents and purposes the ease of the tokenization process and explained, in Bruce's words, its effects and advantages. At the end of the video Bruce says "So as a company, as a stock issuer, securities issuer, you're centralized anyway. Bitcoin purists might say, -Oh my gosh, he just admitted he's centralized.- Well yeah, that's what companies are. Disney is centralized, Apple is centralized. I can issue a million new shares if I want, I can dilute you, I can do every other thing, and that's not a failure of blockchain and it's not a failure of this governance or anything else. That's just the reality of the world. Issuers are centralized. I'm a securities issuer, I'm centralized" [36]. In this way,

[6] Bruce Fenton is the CEO Chainstone Labs/Atlantic Financial and Board Member at Medici Ventures, tZero & the Bitcoin Foundation

having just transformed into a token the shares of his own company, Bruce explicitly denied the first two misconceptions mentioned in section 2.2.1 and, implicitly, also the third. To demonstrate how wrong the third misconception was, later in this chapter, the tokenization process and the actors involved in it will be explained. In this way, the evident advantages that this process can bring will also become explicit.

We start by listing the parties involved in the tokenization process:

- Security Token issuers: companies issuing stocks;
- Trusted third parties: Know Your Customers (KYC), Ant Money Laundry (AML) services providers, accredited investors checking services etc.;
- Security Token Platforms: digital platforms that allow the token to be issued using underlying technology;
- Parties facilitating the exchange: exchanges, OTC desks and similar services;
- Legal: lawyers who help in the decision of who can invest, who make up and write disclosures agreements and file documents with the right entities;
- Software engineers: who write ad audit the smart contracts, playing a vital role for the process;
- Parties included in the whitelists (explained later on in this section) created by the issuing company (accredited investors or established investors).

By analysing two types of tokenisation services, it is easier to explain how the parties involved play a role in the process and how tokens are actually issued in the case of the opening of a company's capital.

Before starting to present the process examples, it is important and preliminary to clarify the concept of whitelist. A whitelist is a list of investors, chosen by the token issuer, who are the only ones authorized to buy, own and exchange (among themselves members of the whitelist) the tokens of those specific tokens.

As a first example, the process of one of the first and most famous security tokens platform is presented: Harbor. This platform offers a digital securities platform for compliant fundraising,

investor management, and liquidity powered by blockchain technology. Specifically, let's take the example of a token issuer that wants to sell a property worth 50 million euros. The process, managed by Harbor, looks like this:

1. Harbor helps the issuer to create the site that shows photos and details of the property to be sold and redirects, in case of interest of a potential investor, to the site of Harbor;
2. Once on Harbor, investors create their own account;
3. Each account created is verified by a KYC/AML provider that works with Harbor (as a third party);
4. Subsequently, the investor has access to all official documents regarding the offering memorandum, investor agreement, perspectives and the documents and information made available by the investor;
5. In case of interest, the investor signs all required documents. The procedure is conducted entirely digitally and online on the Harbor website itself;
6. At this point, we proceed with the payment (in any currency, crypto currency or crypto currency that will then be converted into normal currency) that is verified by an external company (paid by Harbor), which verifies that the payment has taken place and that everything is fine;
7. When everyone has paid, Harbor closes the fund and sends a notification to the investors notifying that the issuer has accepted the investments;
8. Harbor creates the security token, programming smart contracts and emitting, digitally speaking, the tokens on the platform;
9. This is followed by a series of audits of the code and the tokens themselves;
10. The tokens are stored in a portfolio with a qualified Custodian that is assigned to the investor;
11. Finally, there is an educational campaign by Harbor on the investment and operation of the platform. After a fixed time, investors are free to trade tokens between themselves (from the whitelist previously created by the issuer, following his criteria of preference/necessity).

Harbor only takes care of the initial part of the entire life of security tokens and does not deal with secondary trading. It is therefore an important part of the road to unlocking the potential level of liquidity, but it does not manage or provide the entire process. The token exchange can then take place on any other trading platform.

Here are a few sentences from Harbor CEO, which illustrate some of the platform's operational advantages: "So you can think of Harbor as essentially a trade-compliance oracle in the ethereum ecosystem. So that token that has a little bit of a smart contract in it that pings the oracle Harbor, every time that token goes to change wallet addresses, it pings Harbor, and Harbor checks the who and where of the transaction to make sure it's compliant. It checks who the buyer and seller are, it checks what the trade is, and it checks where it's occurring to make sure that all of those matches. If all of those are compliant, no one knows Harbor was every involved, and the trade goes through. If it's not, the trade throws an error and it never happens." and "Users can have multiple wallet addresses, they just simply have to register it with Harbor. So that way we can correlate the blockchain identity with the real world identity. Our expectation is lots of folks will have multiple wallet addresses".

To analyze the second part of the life of security tokens, it is fair to analyze how the process of exchanging tokens on an exchange platform takes place.

In this case, as an example, tZero, an exchange for capital markets, was considered. Here's how a typical tZero transaction goes:

- The seller has security tokens to sell. The tokens are in their possession but, to start the exchanges, they are transferred to a controlled address of tZero and are instantly represented on the seller's account on tZero;
- The seller creates a sell order on the platform;
- The buyers, previously registered to the platform, have ether or currencies and want to buy tokens (of the seller) on tZero;
- Buyers create buy orders on the platform;
- The actual transfer (netting between sell and buy order) does not take place on blockchain but on tZero's internal databases;

- Each actor in the process, can withdraw the securities, ether or money from tZero and (after passing the necessary KYC processes) decide to own their securities through the addresses and associated keys (without the help of any platform, as, for example, done by Bruce Fenton in the example mentioned in the previous section), on their ethereum address (wallet) or on their personal account (for money).

The real added value, not always clear to most, is given by the fact that even if the exchange is managed and "centralized" by an exchange, transactions can only take place through the addresses (wallets) of the whitelist (so addresses that are verified by kyc aml providers and authorized and chosen by the issuer) and then even if the exchange is hacked, hackers could not steal anything but at most could move things between the accounts on the whitelist.

Investors are constantly looking for fairly liquid investments that have a sufficient market depth (because they must be sure that they can easily get out of the investment). All this system, generates and unlocks liquidity especially in two cases

- Private placements (a sale of stocks, bonds, or securities directly to a private investor, rather than part of a public offering);
- Exempt offerings (A securities offering exempt from registration with the SEC is sometimes referred to as a private placement or an unregistered offering).

It is important to remember that, among other advantages, there is that of being able to trade securities at global scale in a safe and fast way. Moreover, it is important to say that when we talk about security tokens we always know the real word identity (it is always verified and it can always be traced back to it) and the security in question always represents a real word asset (which cannot be stolen through hacking) to counteract what happens with crypto currencies. For this reason, even if a security token provider or a platform were to close, its actions (tokens) would not disappear and it would be sufficient to transfer to another platform.

2.3 THE PROCESS OF RAISING AND TRADING CAPITAL

This part will analyze the various methods of raising capital already mentioned in the previous pages. In particular, an explanation of the ICO and crowdfunding processes previously used as comparisons to classical collection methods will be presented. However, these methods are not common among companies with a certain structure and size.

Many successful companies, private and/or characterized by the presence of institutional investors in their capital, find themselves, at a certain point in their life path, considering the possibility of listing on the Stock Exchange. Companies may have a plan of new investments to finance or may want to grow more incisively through acquisitions; or even, members of the founding family or financial partners may seek an opportunity to diversify the investment or face more easily a generational change (willingness to exit the investment). Initial Public Offering (IPO) addresses these needs and is a key choice for the company's future. This requires companies to carefully assess all aspects of listing and the implications of listing on business management. This process has a central part for this thesis and is explained in the last paragraph of this chapter.

2.3.1 CROWDFUNDING

Crowdfunding is a process through which the promoter of an initiative of an economic, social, cultural or charitable nature asks the general public (crowd), through a the portal or a platform (usually on the internet), sums of money, even small amounts, to support the project exposed during the initiative (funding). More technically, it is the practice of funding a project or venture by raising small amounts of money from a large number of people, typically via the Internet and is a form of crowdsourcing and alternative finance. [39]

The first real traces of crowdfunding date back to the second half of the 1990s, when online fundraising for charitable projects began to spread. Subsequently, in the early 2000s, web portals were created within which small loans could be made. One of the first was “Produzioni

dal Basso", an Italian portal forerunner of the concept of crowd financing, launched in 2005. It is, however, towards the end of the first decade of the new millennium that crowdfunding begins to spread substantially, thanks to the emergence of leading platforms such as Kickstarter (launched2 on April 28, 2009) and Indiegogo (launched3 in January 2008). [40]

There are different types of crowdfunding, distinguished by the purpose for which the financial resources are collected, or in relation to the remuneration provided for the lenders ("investors"):

- The donation-based model assumes the collection of funds for non-profit initiatives;
- The reward-based model, which provides, in exchange for a cash donation, a non-monetary reward: the receipt of a prize or an intangible recognition, as a public thanks on the website of the newly established company;
- The lending-based model, which is based on microloans to individuals or businesses in change of an interest on the sum of money lent;
- The equity-based model, which provides for the participation in the share capital of the company and which is currently the only form regulated in Italy by Consob. [41]

Crowdfunding, regardless of its type, has a number of advantages. First of all, it has a number of main characteristics that differentiate it from other types of financing: flexibility, community involvement, the variety of its forms and the democratisation of finance. [42] Moreover, in each of its models can allow you to test the validity of their projects, exposing them to the judgment of the Internet crowd and, therefore, to a multitude of people difficult to reach in other ways. In this way it guarantees a return not so much economic, but more understood in terms of feedback. [43] Moreover, in case the idea is well received by the web, a crowdfunding campaign can become a powerful marketing tool able to effectively build a valid brand image, also increasing the possibility of receiving other forms of funding. Moreover, crowdfunding seems to give designers more control over their projects, which tends to be reduced by more traditional forms of financing. [43] In addition, crowdfunding is often a valid alternative to other methods of fundraising, which are often precluded to those (both companies and individuals) who do not have previous documentation on loans or

business activities. [44] Given the topic covered in this thesis work, it is important to outline the specific advantages of equity crowdfunding (equity-based model) where raising capital (if successful) could have several advantages, such as: pave the way for obtaining other resources even on actual stock exchanges, then within regulated markets.

At the same time, this method of fundraising has several drawbacks, i.e. some contraindications that could turn into risks or limits. The critical aspects of crowdfunding can be examined by type: general disadvantages, regulatory and fiscal disadvantages, cost related disadvantages, disadvantages related to inexperience and disadvantages due to the system-country Italy. The complete lack of control over the public that can access the investment is certainly a point against this method, although very often it helps to achieve the collection target pre-set by the company or for the project. It should also be pointed out that presenting a creative project on an online site exposes us to the possibility that someone may freely take possession of the intellectual property rights of the idea. Moreover, it is not to be excluded the possibility of underestimating the costs or even violating the law without even being aware of it. Problems may also arise with the platform and/or funders. Finally, especially in Italy, the very low digital literacy, the lack of knowledge of online payment systems and the lack of awareness and knowledge could give rise to the fear that the project launched is a scam. In addition, crowdfunders may face: a high cost of capital due, in general, to a fundraising cost of between 4% and 10% and a whole series of additional costs [44]; greater difficulties in campaign management due to the lack of experience in launching a project through crowdfunding and a limited crowdfunding activity outside their national borders (cross-border activity) that reduces the potential market. On the side of the investors/financiers of a project, the main disadvantages seem to be connected: due to phenomena of "herd logic" with consequent imitative behaviour of the crowd, promising projects can also be deprived of sufficient resources, allocating them to projects that are actually less scalable and with lesser potential. [44] Finally, the absence of a clear and unambiguous regulation of crowdfunding and the related taxation, which does not protect either party, weighs heavily in both directions.

In addition to the general disadvantages, equity crowdfunding may also have more specific disadvantages linked to its peculiarities. In fact, investing in a company's equity capital through an equity-based crowdfunding portal exposes lenders to five main problems, almost all of which, however, are largely related to two main types of companies: innovative start-ups and innovative SMEs. The first is the loss of capital, but this is a typical feature of every investment. However, the risk could be greater, since the investment, in addition to all existing types of SMEs, can be made in innovative start-ups and innovative SMEs. Therefore, it may be possible to have realities that have been established for a short time and without a track record of solid results. Hence the possible existence of a higher risk profile. For this reason, some authors believe that the investor should only invest in equity crowdfunding resources that he is willing to lose in its entirety, making this investment a choice of diversification of its investment portfolio. The second problem concerns the impossibility of receiving dividends, but this is specific to smaller companies (i.e. innovative start-ups in Italy) which, very often, cannot distribute profits for a certain period of time (4 years in Italy). Therefore, the possible gain from an equity crowdfunding operation in an innovative start-up in Italy could only occur if you resell your shareholding at a higher value, however, with some exceptions, you can not even trade these securities on other markets. There is, then, the risk of illiquidity of the securities themselves that do not have a real and proper market and, very often, are not properly regulated to allow investors to trade securities in a simple way. The fourth potential disadvantage of equity-based is the "dilution", in percentage terms, of one's shareholding in the company that has financed itself through an equity crowdfunding campaign. In fact, considering that such a model constitutes a paid capital increase, if the company in which the investment was made does not launch other crowdfunding campaigns and the lender of the first crowdfunding campaign does not exercise its option right, then the investor will see his shareholding in that company 'diluted', i.e. reduced in terms of percentage weight. In other words, the lender of the first campaign at the end of the following campaigns would have less weight in terms of votes, expected dividends and value. Last but not least, the disadvantage of equity crowdfunding is the possible lack of experience and expertise in the financial field, which is often detrimental and leads to overestimation or underestimation of the real value of the shares/units of your company.

2.3.2 Initial Coin Offering (ICO)

Initial Coin Offering (ICO) is a crowdfunding tool that bases its operation on the blockchain. The basic idea is that when you propose a new project, you put in advance some tokens that investors who believe in that idea can buy at a more or less arbitrary value, hoping that with the success of the network their value increases. This type of financing recalls the classic crowdfunding, where the lender buys in advance for example the good of the startup, but inserts a nuance more focused on the return on investment, because precisely the value of the token can rise dramatically over time (think of Bitcoin for example).

According to the characteristics of the token and of the blockchain, that the developers assign during the development phase, an ICO can assume different characters: if the token is only a currency, the main reason that pushes the lender is precisely the mere economic return, but if, for example, the token are linked to the right to vote or to participate in the life of the blockchain (for example, if it exploits a consent algorithm of the type of proof of stake) then the lender assumes a role of active node within the network and the service.

Initial Coin Offerings (ICOs) were popular well before the STOs and saw explosive growth in 2017, with more than 1,500 ICOs raising a total of more than $28 billion over the past two years. [45]

Given the nature of the ICO process and the similarity with crowdfunding (non-equity-based) and also given the recent negative aura that surrounds ICOs due to the large percentage of scams associated with ICOs themselves, the phases, advantages and disadvantages of this alternative method of raising capital are not analyzed in detail. Rather, a detailed explanation of the Initial Public Offering will be provided in the next paragraph, which represents the perfect benchmark for the Security Token Offering.

2.3.3 THE INITIAL PUBLIC OFFERING (IPO)

In this chapter we're going to analyze the real value brought by the IPO process since it is a key aspect of this thesis' analysis. The listing on the stock exchange represents a key choice for extraordinary management that creates value for shareholders through a positive influence on all aspects of ordinary management. The decision of launching an IPO, must be based on a careful evaluation of all aspects of the company's business, management, stage of development and prospects and must be made after considering the alternative ways in which the company can pursue its objectives. The circumstances, and therefore the objectives for which a company decides to list, may be multiple. The objectives and therefore the possible future benefits for the company strictly depend on the process and on all the parties which advice the company during the process itself. [49]

The third parties involved during an IPO, provide a service of advice to the company on different issues. Therefore, their action can be seen as an effective training to the company. In addition, these parties involved, give advice to the customer (the company that is about to be listed) and make him aware of the responsibilities that he will have after the placing of shares on the market and the preliminary actions necessary to ensure that the company can function well even when its shares are public in the markets. [46] For this reason, some objectives and therefore value that the company draws from the process of listing on the stock exchange, could be:

- **Expand and diversify the financial sources, also with a view to the planned expansion in terms of new investments and acquisitions**. This means that while control of the company is still held by the control group, the company finances itself at low cost;
- **Strengthen leadership skills by increasing visibility and prestige of the company also at an international level**: the listing generates considerable attention from the media, to the benefit of the image of the company and its products and services;
- **Expand the network of business relationships**, through the preparation of periodic flows of financial communication that have the benefit of maintaining the image of the

company in the economic community and thus increase the opportunities for agreements with suppliers and distributors, joint ventures, as well as new business ideas;

- **Increase the credit standing towards lenders and suppliers**, allowing the use of listed securities as collateral with credit institutions on the basis of the value recognized by the market;
- **Obtain a market valuation that allows to know at any time the value of the company** to facilitate subsequent offers on the market, including capital increases, and mergers and acquisitions, where you can use shares as a form of payment (equity cash);
- **Make the objectives transparent and the results of the management visible**, as a result of the increased mandatory disclosure transparency and the intense financial communication activity;
- **To encourage and motivate management and employees also with stock option plans**, creating a direct correlation between the success of the company and their investment and positively influencing productivity and the quality of work; to attract qualified personnel, thanks to the improved standing of the company;
- **Obtaining tax relief** in the case of quotations with the issue of new shares. [49]

There are also various objectives for the shareholders of the company (pre-IPO) which could benefit from various advantages of listing on the stock exchange such as, for example:

- **Provide liquidity to the shares** by allowing existing shareholders to more easily divest all or a part of their holdings;
- **Realize the entire investment** in the case of presence of an institutional investor;
- **Facilitate the generational turnover**, allowing reorganization of owners without causing the loss of control by the family and possibly more easily allow members of the family shareholder to maintain their share without involvement in the management of the business.

As already said, in general, the listing brings new responsibilities, but at the same time it brings numerous benefits that translate into improved efficiency and transparency of the company,

involving in this project all aspects of business management. [47] It is important, however, that the company takes into consideration the obligations and potentially critical aspects that the listing may involve. These aspects, which vary according to the circumstances and peculiarities of the company involved, are generally identified in:

- **The need to make organizational, administrative and managerial changes with a view to listing**: for example, adaptation of information systems, implementation of a compliant management control system, adoption of principles of corporate governance, communication policies;
- **Sharing of strategic decisions**: some decisions that are decisive for the life of a listed company, such as the increase in capital, the offer of new financial instruments, the definition of new stock-option plans, may require the consent of a large number of shareholders whose interests, opinions and reactions must always be kept in mind, even when their approval is not necessary;
- **Management of maximization of shareholder value and shareholder participation in company profits**: the listing process significantly increases the number of "interest holders" in the company who are fully entitled to participate in the company's positive results, both through the distribution of dividends and by increasing the market value of the shares;
- **Information transparency**: these procedures derive in part from regulatory obligations and in part from the need to maintain and strengthen a relationship of trust with shareholders, without however the need to disclose confidential information from a commercial or industrial point of view;
- **Attention to insider trading activities**: in order to ensure equal information among investors and to prevent the occurrence of insider trading, companies are required to

promptly disclose to the public, (in Italy they have to report to Borsa Italiana[7] and Consob[8]), information on facts likely to influence the trend of prices;

- **Susceptibility of the stock to market conditions**: the value of the stock may be affected by the economic phases of the market, as well as by speculative actions, regardless of the management and strategic policies of the company;
- **Management time to devote to the listing process**: even before selecting the team of consultants to handle the entire operation, the company's management will have to prepare to invest a significant amount of time and resources in defining in advance a business plan in which the strengths and weaknesses of their company are highlighted. Throughout the process, you should work with the team of consultants to make decisions that are critical to the success of the IPO. During and after the listing he should also be available to introduce the company to potential investors and to dialogue with market participants. [49]

After analyzing why third parties in the IPO process are so important and the advantages and responsibilities that the process entails, in the next section the process itself and the parties involved are showed.

2.3.2 THE IPO PROCESS AND ACTORS

The preparation for the listing requires the assistance of a team of specialized consultants with whom the company has the utmost confidence and with whom it establishes a fruitful cooperation. Below are analyzed, point by point, the roles of third parties involved in the

[7] Borsa Italiana is a company that manages the Italian financial market, commonly known as the Milan Stock Exchange which was founded in 1808.

[8] The National Commission for Companies and the Stock Exchange (better known by the acronym CONSOB, is an independent administrative authority with an autonomous legal personality and full autonomy whose activity is aimed at investor protection, efficiency, transparency and the development of the Italian securities market.

process and will then present an explanation of the process itself with the major issues and costs. [49]

The main parties involved, besides the company, are:

- **The sponsor**: a crucial figure in the team of consultants who deserves special attention. The sponsor is a financial intermediary who assists the company in carrying out the entire listing process and also for a period after the IPO. It also acts as a guarantor to the market for quality and investment opportunity. In most cases, the sponsor also acts as the global coordinator of the offer, i.e. he also undertakes to place the securities of the listed company on the market. Depending on the expected size of the placement, the company may also appoint more than one global coordinator. Because of the central role it plays during and after the listing process, the global sponsor/coordinator must be carefully selected;
- **Financial advisor**: collaborates with the company and the sponsor in the implementation of the feasibility study, independent preliminary assessment, drafting of the prospectus, preparation of the budget and business plan, instruction of the files;
- **Independent auditors**: responsible for auditing the company's financial statements for placement purposes, for issuing comfort letters in relation to the prospectus and for reporting on the financial statements;
- **Law Firm**: may be appointed by the global coordinator, the company and/or the selling shareholders and is responsible for assisting the company in the statutory adjustments, drafting of the prospectus, legal requirements, share subscription agreements, issuing of legal opinions, etc.. It is therefore necessary to verify in advance the experience of the lawyers, both in terms of familiarity with the legal aspects of the share placements, and in terms of knowledge of the problems of the company;
- **Communication consultant**: is responsible for maximizing the acceptance of the stock by investors through the effective communication of the image of the company and its products, also ensuring the proper management of relations with the press. It plays a crucial role in the marketing phase of the offer, providing investor relations services and "educating" the company to manage relations with the financial community.

- **Tax advisor**: allows the company to optimize the tax leverage, also in light of the new rules on taxation for listed companies;
- **Supervisors**: have the supervisory authority and control over companies and markets, who are responsible for clearance, the publication of the prospectus information functional to the offer;
- **Post-trading services companies**: companies which provide pre-settlement, settlement and custody activities, and offer collateral management services on domestic and cross border securities, as well as issuing services for domestic and international companies. [49]

The IPO process presents always the same type of consulting companies, institutions and third parties involved in the process, approximatively the same time for the completion of the process and same fixed fundamental requirements. Obviously, depending on the geography and the local laws, the process may vary. For these reasons, it has been chosen to illustrate and use the Italian IPO process for the comparison, scope of this thesis. The following figure (Figure 7) shows the entire IPO through the Italian Borsa Italiana, with the estimated time for each part of the process. It is important to specify that the figure shows the minimum time required for each step and thus the minimum time needed to complete an IPO in Italy. [49]

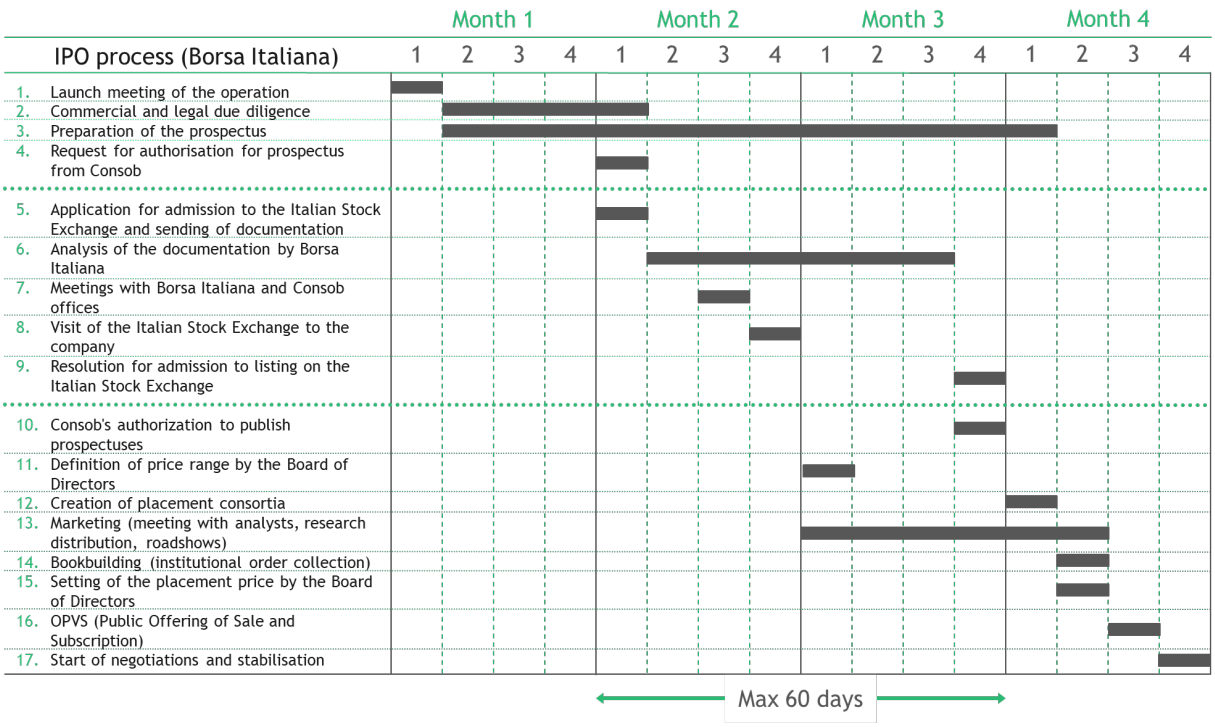

FIGURE 7 : GANTT DIAGRAM OF THE IPO PROCESS IN BORSA ITALIANA

Here below, a brief but complete explanation of each phase of the IPO process:

- **Board of Directors' resolution and appointment of the team of consultants**: the management presents to the Board of Directors the listing project accompanied by the feasibility study. After the Board of Directors has resolved on the application for listing of the company, the ordinary Shareholders' Meeting or, if an increase in capital is envisaged, the extraordinary Shareholders' Meeting is called. Immediately after the resolution of the Shareholders' Meeting, the sponsor, the legal advisor, the auditing firm and the other advisors who will follow the company during the listing must be appointed;
- **Launch meeting of the operation**: this is the first meeting in which the company's management meets with all the appointed consultants. During this meeting, the respective responsibilities are assigned and the timing of the listing procedure is planned, identifying the main steps;
- **Economic, financial and legal due diligence**: the sponsor and the consultants must carry out an in-depth analysis of the company, identifying its critical success factors

and all the necessary elements for an assessment of the feasibility of the listing and the value of the shares to be issued. At this stage starts the drafting of the prospectus and the preparation of documentation relating to the meetings of the Board of Directors and the Shareholders' Meeting;

- **Drafting of the Prospectus**: this is the official document for soliciting public savings. It is prepared by the sponsor (according to the schemes required by Consob), together with the company's management and legal advisors, on the basis of the results of the analyses carried out during the due diligence process and is intended to provide all the information regarding the company and the structure of the global offer. This document contains data relating to the economic and financial condition of the company and its performance; it also describes its position vis-à-vis its competitors, its management, objectives and strategies. Other factors that are analyzed are: the workforce, suppliers, customers, creditors and all contracts, so as to ensure investors that financial reports are accurate and adequate. In addition, there are sections dedicated to information about the solicitation and the financial instruments covered by the solicitation. The final version of the prospectus is filed with Consob, which will have to issue the authorization for its publication;
- **Admission to listing by Borsa Italiana**: within two months of the submission of the application, drawn up according to the specific form set out in the "Instructions to the Regulations", Borsa Italiana resolves and informs the issuer of the admission or rejection of the application, simultaneously notifying Consob and making the decision public by means of its own Notice. The effectiveness of the admission measure is valid for six months and is subject to the filing of the listing prospectus with Consob;
- **Publication and distribution of the stock search report to analysts**: research is a very important factor in determining investors' opinion about the company's positioning and valuation. It aims to communicate the investment case of the stock and create momntum during the pre-marketing phase when it provides analysts with all the necessary elements to express their opinion. It contains a detailed analysis of the company and the business, a presentation of the structure of the offer, a description of the valuation methodologies used and is the main source of financial forecasts;

- **Creation of placement consortia**: the global coordinator, who generally also acts as a sponsor, forms a consortium with other banks with the aim of accumulating "declarations of interest" from institutions and brokers in order to subsequently determine the final number of shares and their allocation among investors;
- **Pre-marketing**: Analysts from the banks of the placement consortium informally meet potential investors to present the company and distribute the research they have elaborated in order to form an opinion on a possible preliminary price range for the IPO. In addition, during this phase, investors have the opportunity to express their negative perceptions and doubts and to become familiar with the company while banks can identify candidates for one-on-one meetings;
- **Roadshow**: aims to increase interest in the company's investment case. The top management of the listed company participates in a series of meetings in major international financial centers, during which it presents itself and the company's key data to potential investors. A roadshow requires a lot of energy, especially in terms of the time that management must be willing to spend. If well organised, it gives the opportunity to meet institutional investors even in one-on-one meetings and to express their skills, demonstrating their commitment to maintaining regular contact with the financial community and thus positively influencing the offer price, to the benefit of raising capital;
- **Bookbuilding**: potential institutional investors communicate to the book runner the amount of securities they intend to buy and the price they intend to offer and, on the basis of the orders collected, the price and the quantity of offer of the placement is fixed. The bookbuilding mechanism allows to determine the highest price at which the securities can be placed to institutional investors;
- **Price fixing process**: it usually happens in two steps:
    1. The Shareholders' Meeting approving the capital increase shall set a preliminary price range sufficiently wide to take account of any changes in market conditions. This preliminary price range may be restricted by the Board of Directors in the run-up to the launch of the transaction;

2. On the basis of the bookbuilding results, the placement price for the launch of the OPV(S) is determined, in the case of a fixed-price public offer, or the maximum price is determined, in the case of an open-price public offer.

- **OPV(S) Public Offering (and/or Subscription)**: the shares are assigned to the members of the placement consortium who will take care of the indistinct public offering, the duration of which is at least two days. Within 5 days from the end of the public offer it is necessary to make the payment and to deliver the shares by means of the deposit to the post-trading service company or companies;
- **Start of negotiations and stabilization**: during the first day of official trading the market price of the title which is an important signal the interest of the operators in the of the company. After the first day of listing there is often a period of price stabilization of the title, usually 30 days, during which the consortium reserves the right to to intervene in the financial market in order to to support its development also through the use of the greenshoe [9]option, if any in the structure of the offer. This operation is also used to to answer any major question by investors.

Later on, in the finding section, it will be explained if the DLT technologies is able to bring improvements in this process adding value and, at the same time, eliminating part of the parties involved in the process or parts of the process itself. [49]

Given the importance of the big step that a company takes when it is listed on the stock exchange, there are certainly some stages of the process that are much more important than others and, in most cases, represent those with the greatest added value. [48]

IPO's phases value analysis

The very act of evaluating the value of a company implies, implicitly, various actions with added value for the company which, in order to obtain the highest possible valuation among those present in the "valuation range", carries out various preparatory actions and

[9] The green shoe, also known as the over-allotment option, is an option that allows the issuer to increase the size of the offer in order to respond adequately to the demand for securities by investors when placing the securities of a company, with the aim of entering the stock exchange.

transformations considered necessary for the listing. The following is the process of defining the price of the company that has four macro-phases:

- Valuation carried out at the time of the pitch by the bank: deliberation of the company's board of directors and appointment of the team of consultants while the management presents to the board of directors the listing project accompanied by the feasibility study. The Board of Directors meets to decide on the appropriateness of the listing and, once resolved, the ordinary and, if necessary, the extraordinary shareholders' meetings are called (for a capital increase). After the resolutions of the shareholders' meetings, the sponsor and the other consultants who will work alongside the company (already described above) are appointed.
- Valuation carried out in the phase of due diligence: It takes place in the first month of the public offering and consists of an analysis of a company/activity by a group of experts in order to highlight the strategic aspects, business aspects, future prospects and financial results of the company. The primary purpose of the listing is to raise financial resources on the capital market and therefore a sequence of activities is initiated to subscribe to the financial instruments of the listed company.
- Pre-marketing and identification of the indicative range of price: Analysts of the banks of the placement consortium meet informally with potential investors to present the company and distribute the research they have elaborated. During the pre-marketing phase, the investment bank conducts a survey of institutional investors, which leads to the definition of an indicative price range. Only at this point can the bank, in possession of feedback on the price that institutional investors are willing to pay, compare with the issuing company and any selling shareholders and arrive at the definition of the target range and the "maximum price" or the reference price for the next phase, i.e. the collection of orders from investors. After the pre-marketing phase, the company proceeds with the roadshow and book-building.

- Pricing: divided into two phases: 1) the shareholders' meeting that approves the capital increase sets minimum and maximum price thresholds that are sufficiently distant from each other to take account of any changes in market conditions; 2) on the basis of the results of the book-building, the placement price is determined in the case of a fixed-price public offer, or the maximum price is determined in the case of an open-price public offer. [48]

In the first phase, during the launch meeting of the operation, where the management meets with the team of consultants in charge, there is the assignment of their respective responsibilities and the planning of the timing of the listing procedure. This gives the management more responsibility and brings a profound change within the company. All employees, aware of the imminent listing, will be more responsible by understanding what it means to open up to markets and international investors. The company is more exposed and therefore the transformation of many of the internal processes, starting from auditing, information verification, compliance etc. moves and changes the attitude of management and employees bringing real added value to the company.

Following the same principle, the evaluation process itself also brings much added value. Consultancy and surveys conducted by professionals outside the company but involved in the process, lead to the definition of an evaluation range and involve training of management and staff that adds value to the company. Added value that is not present in other fundraising processes where these intermediaries are not present.

it is very curious that, as shown in figure 8, over time the company's evaluation and pricing process leads to defining a more precise and lower price than the maximum identified in the initial range, while, in the same period, the added value brought by the consultants and by the

process itself to the company grows continuously.

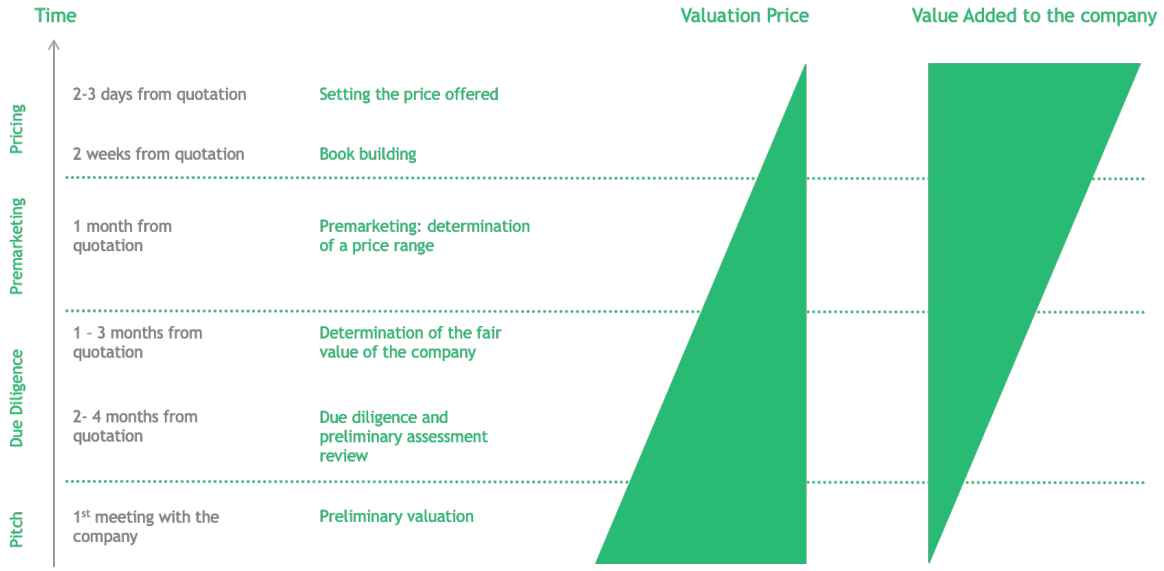

FIGURE 8: ADDED VALUE OF THE PRICING PROCESS

Does the same added value apply to fundraising through the use of blockchain technology? In the next paragraph we try to hypothesize the way in which the DLT can impact the IPO process just described and try to define what, according to the literature, are the parts of the process that, not adding added value, will be probably eliminated.

2.3.4 Impact of the DLT on the IPO process

Despite the limited literature of reference, one can try to define the impact of blockchain technology on capital raising and the IPO process in particular, by analyzing the opinion of the experts in the field Blockchain and their vision on the future of security tokens. It could be taken in analysis the case, already showed, of the listing process on the Italian stock exchange. According to what has already been stated on the future visions of the security tokens [37], the greatest impact could be on the parts of the process which are more easily automizable and therefore on those which concern the verification of the requirements and the compliance. This would result in the loss of a large part of the activities of some third parties such as institutions, legal advisors and all post-trading platforms. The blockchain experts are

very confident about the potential of security tokens, however, professionals from investment banks and financial advisors are not as convinced about the elimination of these participants. [37]

Taking as an example the steps from 5 to 10 described in figure 7, it could be hypothesized the elimination of these since the entire process of verification and compliance could be automized and take place thanks to the technology already explained (smart contract). In this case, the effectiveness of the technology would replace the efficiency of the current process and would improve times and procedures conducted until now by human actions. The value added by the parties involved in those phases can be considered as very small. The same hypothesis is valid for the post-trading phase. The next chapter will analyse, in details, the post-trading phase and the possible scenarios generated by the European Union view.

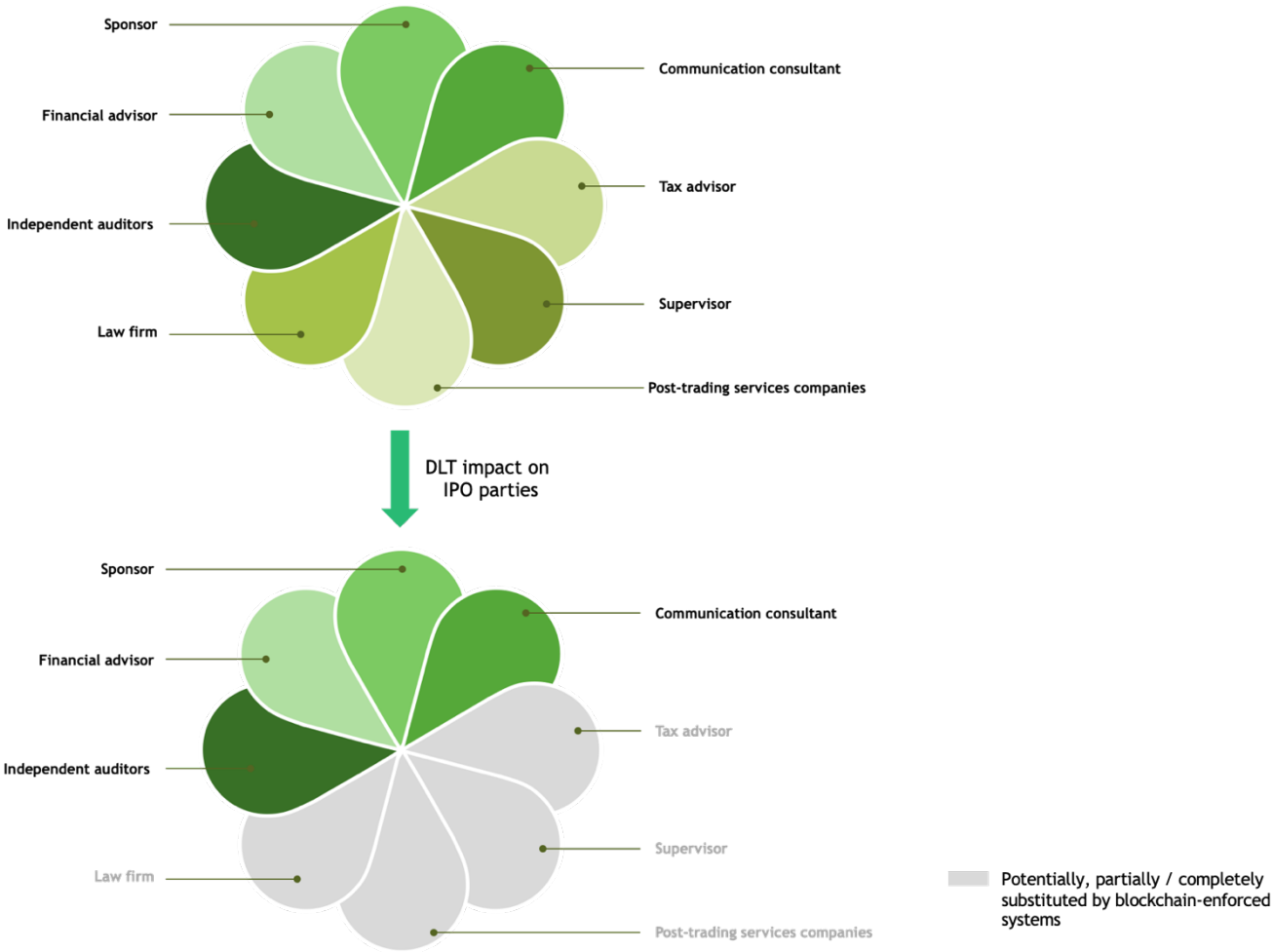

FIGURE 9: EFFECT OF THE DLT ON THE IPO ACTORS

In general, the total impact that the technology could have on the actors involved in the stock exchange listing could be that illustrated in Figure 9.

However, the experts are still not sure that any elimination of one of the parties involved can be fully replaced with the same effect on the company that you want to quote. This is because, despite the obvious effectiveness of replacing some man-made processes with automated ones, any contact with consultants of any kind could, generally speaking, bring added value in the form of advice or suggestions on how to act in the future after the listing. Potentially, some of the players could disappear and also remove some of the added value that these (mainly consultants) bring to the company during a normal stock exchange listing. [37]

2.3.5 DLT IN SECURITIES POST-TRADING, THE EU'S VIEW

Here below it is explained the European Union's (EU) view about the potential of the DLT technology in the first part (which is the only interesting part of the process for the scope of this thesis) of the post-trading process.

EU perspective

The financial sector has developed over time as a network of mutual trust institutions, characterized by legal agreements and regulated procedures in order to avoid risks, such as operational and counterparty risks, that are not directly linked to the activity of a securities issuer but concern the entire financial sector. The regulatory authorities shall supervise the trading of each institution and its responsible and authorized counterparties. This creates scope for the implementation of restricted DLTs among market participants. However, the characteristics of the blockchain, which are so important for the Bitcoin network (pseudonymise of market participants, immunity from supervisors, copies of the ledger being accessible to anybody all over the world, and irreversibility of unlawful transactions), are in fact not relevant for the financial sector. Market participants need a system that is compatible with the standards they are required to meet such as, for example, implementation of the

know-your-customer (KYC) rules, transparency and accountability to regulators, respect for the rule of law and confidentiality of trading strategies. It also matters that everything listed above is relatively cheap to maintain.

Leaving aside for a moment the description of the vision of the EU, also published in 2016 and considering how much in just a few years such an industry can evolve, it is right to point out that in recent years several realities have arisen, in the DLT world, which have immediately paid attention to the needs of the financial markets mentioned above. Some examples of these are the start-ups mentioned in the previous paragraphs which, although committed and focused on possible new ways to raise capital, consider the processes of KYC and AML as a major part of their system.

Problems with the present post-trading system and considerations on potential improvements through DLT technology

The lack of interoperability between centralized database systems limits direct processing for a number of non-vertically integrated financial institutions. In addition to extending the settlement cycle and increasing the cost of back-office procedures, the need to reconcile accounts held by different intermediaries creates some risks, such as: settlement failure chains (as late settlement of a transaction can affect the settlement of transactions with third parties), human errors (as the system is sometimes reconciled manually) and limited flow of collateral.

Currently, financial intermediaries keep several separate records of the same information (as already explained for the US system). Banally speaking, it is thought that TLDs could save money in back-office activities by avoiding duplication of data. But, of course, this is not the case since data redundancy is maximized (which is very useful for reacting to cyberattacks) since each node keeps a copy of the register or a part of it. The real potential advantage of using DLTs lies in the fact that you would avoid the redundancy of business processes and the various steps between financial intermediaries, since a copy of the register, always updated and secure, would be available to everyone at any time.

To today date, financial intermediaries have to update their accounts each time a new transaction is made. They are therefore required to send all relevant results of this exercise to stakeholders at different levels of the post-trading industry so that they can reconcile their accounts to reflect the new situation and inform stakeholders of any changes. The securities flow between trading and settlement takes time, (as already explained for the US system), although execution of the matched settlement instructions at the settlement level can be instantaneous.

Current process and possible scenarios

The diagrams below (Figures 10, 11, 12, 13) present the current picture of the security of a securities transaction between end investors (left) and three potential scenarios identified by the EU that identify how the picture could become as a result of a multi-level integration of the TLD (right). Below is a brief description of the current process and below (following paragraphs), considerations and analysis regarding the parts of the process on which the DLT technology could have a real impact.

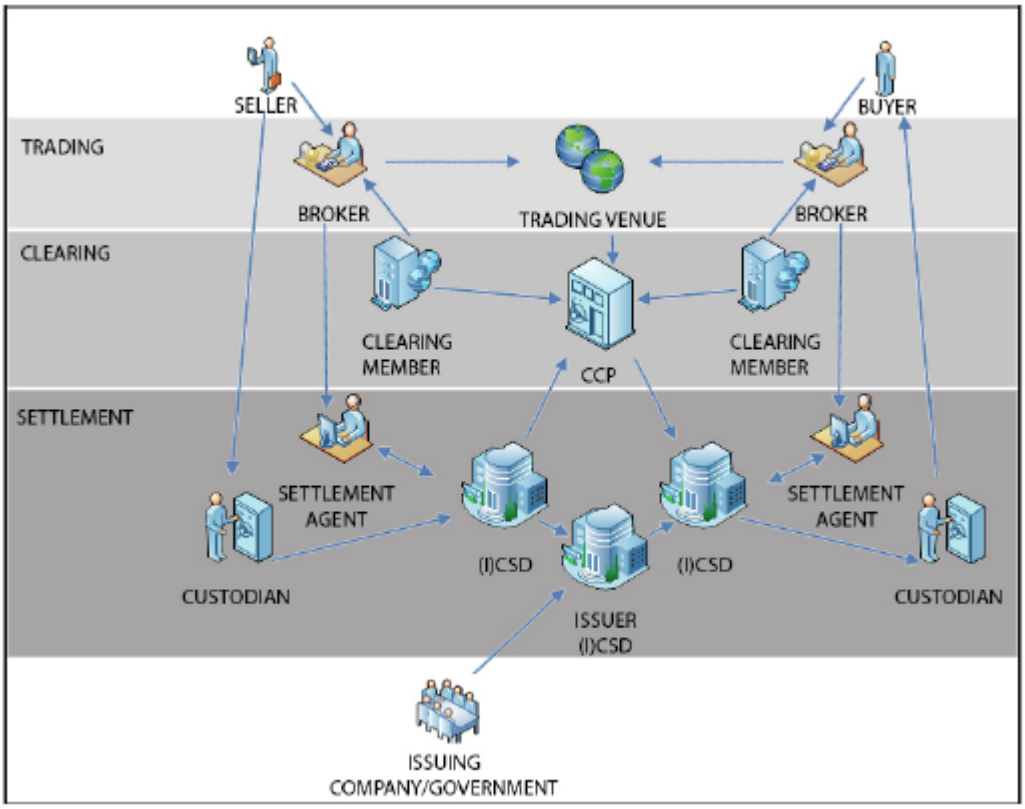

FIGURE 10: POST-TRADE PROCESSES IN THE SECURITIES LEG OF CURRENT TRANSACTIONS

From the outset, the process may be simplified by using either internalized settlement (when both end-investors have their accounts with the same custodian) or via consolidation among intermediaries, e.g. the clearing member and the settlement agent could be one and the same entity, which sometimes also acts as a custodian for end-investors. Consolidation may, however, lead to a lack of interoperability which may lead to anti-competitive behavior, in particular in the case of market infrastructures constituting natural or regulatory monopolies.

The buyer and seller must instruct their respective intermediaries as to their willingness to trade. Orders are forwarded to a trading venue where they can "cross" in the order book or on an alternative trading system and enter into a transaction. The details of the transaction are often sent to a clearing house which reconciles the orders, possibly offsetting them with other pending instructions, in order to reduce the outstanding positions of its members. The clearing house can then, in some cases, become the central counterparty (CCP) for both end-investors (in which case the process is known as "netting by novation"). Perhaps, at the same

time, clearing members inform their respective intermediaries of their obligations and brokers instruct their settlement agents. The settlement agent of the seller's broker receives the securities from the seller's custodian to his account and credits them to the clearing house - which, for simplicity, is supposed to have accounts in both central securities custodians of investors (CSDs). The clearing house then gives instructions for the securities to be credited to the account of the buyer's settlement agent, which credits them to the buyer's custodian. Reconciliation between the investor's CSDs and the issuer's CSDs may be necessary, for example to allow notarial and asset servicing functions. Any of these steps may require that the records of one party be reconciled with those of other parties at different levels of the value chain.

Here below the three possible scenarios individuated from the EU:

- **Scenario 1:**

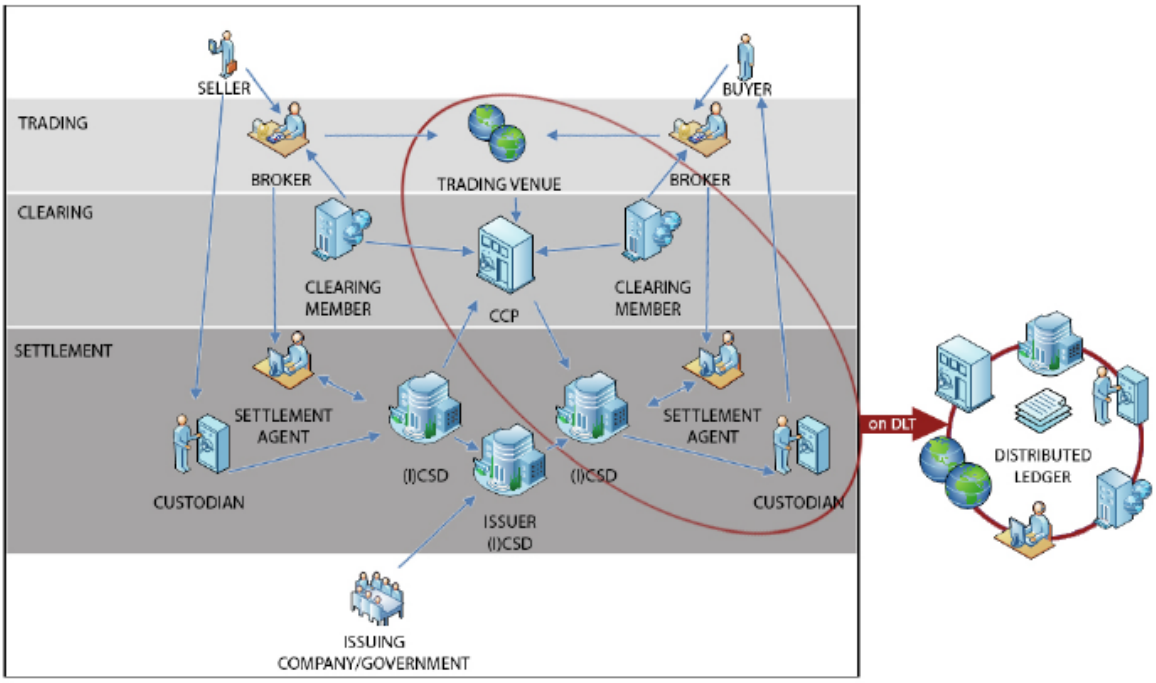

FIGURE 11: HOW DLT COULD AFFECT THE EFFICIENCY OF POST-TRADE IN THE SECURITIES

A part of post-trade institutions (on the buy side of this diagram) may develop their own DLT for internal use. All business relations inside the red circle would then take place as straight-through processes on the distributed ledger.

- **Scenario 2:**

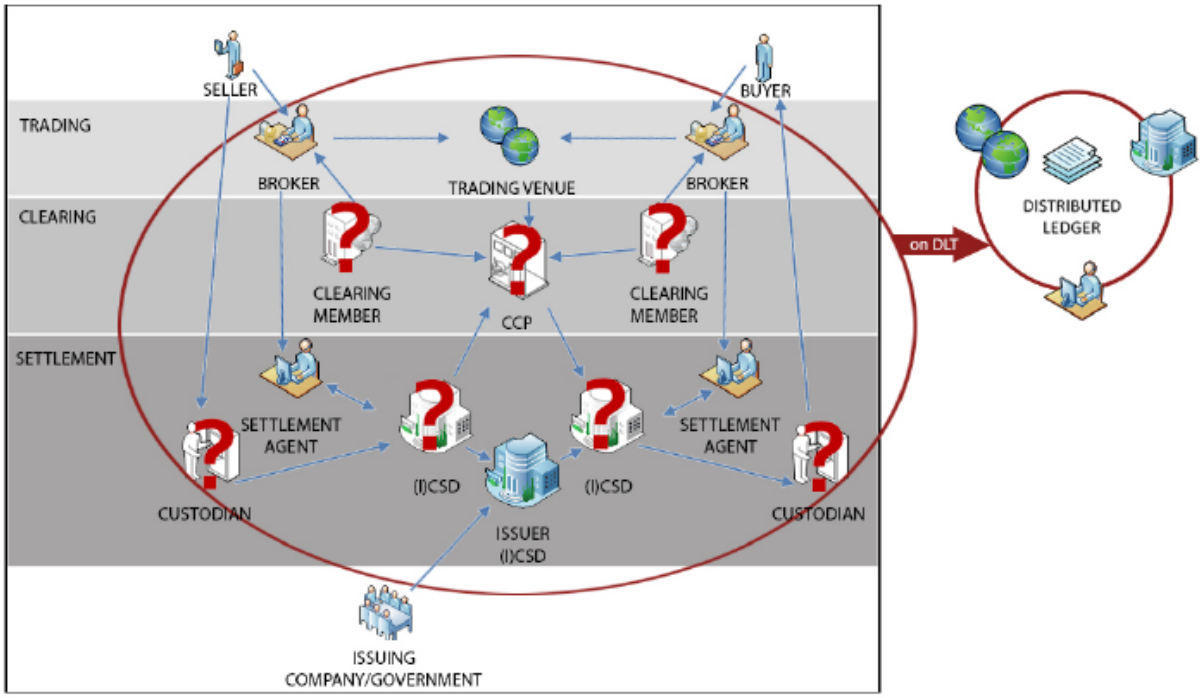

FIGURE 12: HOW A MARKET-WIDE DISTRIBUTED LEDGER MAY AFFECT THE POST-TRADE LANDSCAPE OF SECURITY MARKET

If the whole post-trade industry migrated to a distributed ledger settlement process, securities accounts would be updated automatically. Depending on the extent of the implementation of smart contracts, some layers of the industry could become redundant.

- **Scenario 3:**

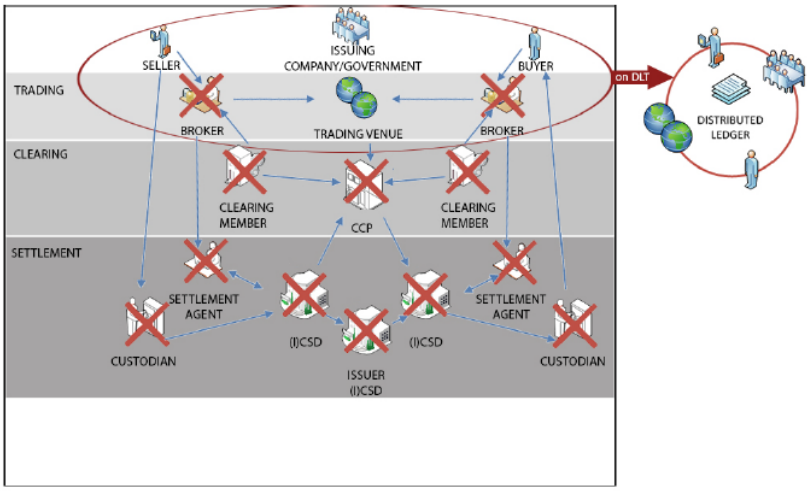

FIGURE 13: HOW A PEER-TO-PEER MARKET FOR SECURITIES BASED ON DLTS COULD AFFECT THE POST-TRADE

If capital markets were to migrate to a peer-to-peer model, the whole chain of intermediaries would become redundant, and companies or governments could issue their own securities on the distributed ledger. This scenario reflect perfectly what is happening right now in the security market thank to security token movement. And for this reason is the most interesting for the purpose of this thesis.

Impact on the first layer of the process

To conclude, will be exposed, only the impact of the technology on the first layer (Figure 10) and on the settlement layer. The rest of the analysis conducted by the EU on the other layers of the process goes beyond the scope of this thesis and will not be reported.

Seen the system created during the years, the notarial function has assumed such an importance that many national markets entrust to a regulated monopolist the task to guarantee the integrity of the issues of securities and the regulation of its operations. According to the EU, this will remain a key role even if DLTs are adopted, as "a reliable institution will be needed to ensure that the number of securities registered in the distributed register matches the description of the issuance provided" (Pinna, Ruttenberg, 2016).

Due to the different interests and economic incentives of the parties, the role of notary cannot be delegated to issuing companies or governments and therefore a third party is necessary to perform this function. The third party would ensure that only the amount of securities publicly issued is traded, with no unwarranted dilution of investors' claims since "Confidence in the claims that securities bear over the underlying real assets is fundamental to allowing both corporate financing in the primary market, and maturity transformation, storage of value and hedging in secondary markets" (Pinna, Ruttenberg, 2016).

Although the participation of regulatory and control bodies will still be required, the validation and therefore the settlement of transactions could be delegated to nodes managed by a number of market participants. However, this could cause problems regarding the confidentiality of transactions (a key issue for investors) since an efficient validation of transactions in a DLT currently requires validators to access the details of the transaction to verify its validity. Since this issue is very important for investors who want to keep their trading strategies confidential, it is very likely (according to the EU view) that interest will shift to DLTs using zero-knowledge[10] proof protocols.

The last feature analyzed and presented by the European Union concerns the security of the system at this stage of the process and what it could become when the DLTs come into play. The impact of the DLT on IT resilience would not only depend on the protocol of the DLT in question and therefore on its validation method, but on more characteristic aspects of the general architecture of the system itself. In particular, an improvement in security could be brought about by the fact that, in the event that each node has the security features of the centralized databases currently used for regulation, an attacker would have to control a number of these IT systems (rather than just one) to influence the system. Therefore, the ability of individual nodes to withstand attacks will be equally important. However, the validation role is and will be distributed among "institutions" less cyber-aware, so it is difficult to see right now whether the final impact of DLTs on system security will be positive or

[10] Zero knowledge Protocol is a method where one party can prove (prover) to another party (verifier) without revealing knowledge of secret itself. (Ashish, 2018)

negative. In both cases, the redundancy of copies of the distributed ledger kept by the different participating institutions can facilitate recovery in the event of system failure.

3. METHODOLOGY

After defining the research question following the literature review, this chapter will introduce the research methodology, explaining in more detail the research design, the sampling method, the data collection and the way the analysis was conducted. The chapter also outlines the strategies used to ensure the validity and reliability of the analysis. The step-by-step model of the Mayring research process (2014) was used as the framework for this thesis and guideline.

FIGURE 14 : STEP-BY-STEP GUIDE OF THE RESEARCH METHOD

3.1 RESEARCH DESIGN

Given the small number of texts and literatures written about security tokens and the application of DLTs to the world of capital raising, a qualitative and explorative-descripting research design was chosen. The focus of a qualitative research approach is to explore and understand the meaning individuals or groups ascribe to the research issue [30]. This can be done through the analysis of interviews, focus groups, observational studies, document analysis or secondary analysis [29]. For this thesis, semi-structured expert interviews were chosen to elaborate on the phenomenon.

In qualitative content analysis two different approaches can be followed: explorative or descriptive research design. When choosing the descriptive design, categories are defined beforehand based on existing theoretical ideas and their existence will be checked through an

analysis of the interviews. Explorative design follows an inductive approach, where new categories will be formulated, based on the information collected during the interviews. Then, through continuous comparison of the transcripts, concepts or approaches are emerging (Mayring, 2014). On the basis of the research question and the fact that so far the topic has not been treated by a sufficient number of texts, a descriptive-exploratory approach will be followed (i.e. a mix of the two approaches) and an inductive framework will be built, based on the analysis of the interviews.

3.2 SAMPLING

In order to conduct the analysis, it was necessary to identify the best professional profiles for conducting the interviews. In the qualitative analysis of the contents, the interviewees must be chosen in such a way as to ensure that they can contribute to the research topic [30]. In this case, the experts were selected on the basis of their professional experience and suitability for the research problem [31]. Experts are professionals who have in-depth knowledge or long-term experience on a given topic and, as a result, give rapid access to unexplored areas [32]. In this case, the main condition was that the selected applicants had to be familiar with the DLT technologies and funded processes and in particular with those concerning stock exchange listing and capital raising. Given the strong correlation with the legal aspect of the issue and the different legal landscapes between the various European and non-European countries, the partners interviewed were chosen by different companies and countries [33]. The specific condition was that they were familiar with the application of DLT technologies in the financial sector. The interview partners were identified and contacted through the private network or contacted on the LinkedIn platform or by email. In addition, the interview partners referred to other participants. The sample consisted of 9 experts from different companies in the fields of fintech, Distribute Ledger Technologies, investment banking and private equity (Figure 15).

Name	Company	Position	Location	Description
Luigi Bruno	-Deloitte	-Senior Consultant (Cyber Risk)	Zürich (Switzerland)	*"I am a multilingual legal counsel holding civil and common law degrees, with experience in Private Equity/VC and Blockchain/IT/Cyber Risk, in-house, at a Tier-1 international law firm and in a Big Four. I actively invest in early-stage tech startups, lead a Rotaract Club (Zurich International) and frequently co-organize and speak at major legal and tech conferences worldwide. I can code in Python, HTML, PHP and Java, am a Corda Certified Developer and have a very deep knowledge of Distributed Ledger Technologies and Smart Contracts"*
Raffaele Battaglini	-Battaglini - De Simone Law Firm -Vernero & Partners -JUR	-Founder -Of Counsel (Corporate Law) -Chief Legal Officer	Turin (Italy)	*"I assist entrepreneurs, companies and startups in the internationalisation and innovation phases, business aspects which I am acquainted with since my postgraduate LL.M. degree in Innovation, Technology and the Law at the University of Edinburgh in 2006. I am currently involved in blockchain-related projects and ICOs. I also advise established companies and digital startups in the legal aspects of new technologies, commercial contracts, M&A deals and corporate matters including international corporate structures, due diligence, open innovation deals, e-commerce and app development. My experience is both as an outside legal counsel and in-house lawyer. I currently hold the following roles: - Co-Organizer of Legal Hackers Torino, the first Italian chapter of the global movements of lawyers and innovators; - Secretary General at AGICONSUL - Legal Experts and Consultants Association - member of CONFINDUSTRIA Innovative and Technological Services where I am also in charge of the organisation of events on international trade and innovation"*
James Bevilacqua	-AmaZix	-Senior Manager Controlling and Compliance, DPO, Management and Business Advisor	Turin (Italy)	*"Managing the controlling and compliance topics at AmaZix, mostly related to the Cryptocurrencies accountancy, treasury and change rates. GDPR, Internal controls, ERP, accounting methods, financial reporting, law and taxation, are the areas in which I support directly and advise the AmaZix Executives. Previously experiences in the automotive, TMT and consulting industries"*
Enrico Ferro	-United Nations -ISMB	-Member of the Expert Group on Blockchain -Head of innovation development department	Turin (Italy)	*"C-level Strategist, Innovation Advisor, PhD Scientist, Angel Investor, Head of Innovation Development Department at ISMB"*
Partner (Anonymous)	-Leading Italian mid-market investment bank -Start-ups and SMEs	-Partner and Managing director -Investor	Milan (Italy)	*"Professional with over 20 years of experience in closing M&A deals and stock exchange listing transactions of medium sized companies. Business angel and investor in the fintech sector"*
Michela Agostini	-Fineurop Soditic	-Associate	Milan (Itraly)	*"Together with my colleagues we manage M&A and debt advisory operations in the Italian market. My focus is on debt raising operations, but also valuation and compliance operations for M&A deals, capital increases and IPOs"*
Associate (Anonymous)	-Ardian	-Associate, Private Equity and market practices	Milan (Italy), Paris (France)	*"After various experiences in the world of fintech and investment banking, I am now associated with a major French private equity fund. My job requires me to be constantly updated on new technologies, such as the blockchain, which we use to grow and improve many of the companies in our portfolio. In addition, I am very well prepared on the processes of mergers and acquisitions of companies, buyouts and IPOs, useful for the growth of companies in the portfolio and the process of divestment and exit that we have to deal with as an investment fund"*
Vice President (Anonymous)	-Equita SIM	-VP	Milan (Italy)	*"I'm a Vice President at Equita SIM which is an independent Italian investment bank, a reference partner for companies and institutional investors, with over 45 years of experience. Independent advice and in-depth knowledge of the markets accredit Equita with national and international institutional investors, ensuring a unique positioning in the Italian market, with a focus on mid & small caps. Equita carries out its activities through different business lines, highly synergistic and supported by a research team recognized as one of the main players in the Italian market"*
Former Analyst (Anonymous)	-Advance SIM	-Former Analyst	Milan (Italy)	*"I'm currently an M&A analyst in a leading American investment bank in London, but before that I used to work for Advance SIM focusing on several IPOs. During my experience I had the possibility to discover all the critical phases of the IPO and to master the process from the investment banker perspective"*

FIGURE 15 : TABLE OF INTERVIEWED PROFILES

3.3 DATA COLLECTION

The primary data were collected through semi-structured and in-depth interviews with experts. Semi-structured interviews allow respondents to ask and answer questions in an informal and flexible way and to suggest discussion points even if apparently far from the topic. The interviewer can adapt to the interviewee's answers and some topics can be highlighted or clarified. Additional unexpected or unsolicited information may be shared [32]. Previously, a list of general questions and topics for interviews was prepared, which was used as a guideline throughout the interviews. However, in order to capture the skills and all the insights of the participants, the interviews were very open, creative and adapted according to the responses of the respondents. The interviews were aimed at understanding, if and when the respondent was an expert on the topic in question, with the intention of asking, later, his opinion on the subject and his vision of the future of the topic. The interviews were conducted on Skype or by phone in May 2018. The duration of the interviews was 30-60 minutes. The interviews were conducted in Italian or English to give experts the opportunity to express themselves without language barriers. All interviews were recorded on tape. A scheme with the most important questions (the four pillars of each interviews) is provided in Appendix A.

3.4 DATA ANALYSIS

Data analysis followed an inductive category development procedure in order to identify key areas and aspects of the material. In this way, the analysis of the text allows to take into account only those parts that refer to the question of the research. Inductive approaches by category aim to discover categories that derive directly from the interviews themselves without considering previous theoretical concepts [29]. Since the research question is an exploratory question, the categories have not been defined in advance. A category is a significant concept that is assigned interview quotations. The aim is to reduce the complexity of the material without losing focus on the main idea. According to Mayring (2014), "this

reduction produces a clear overview of the data and helps to identify models". The process followed for the inductive development of the category is shown in the Figure 16 below.

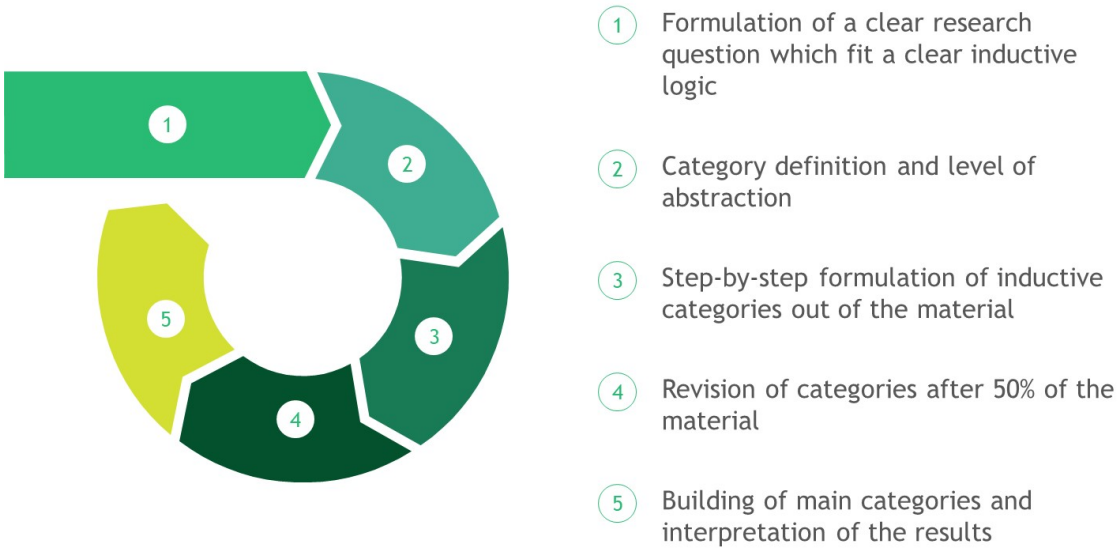

FIGURE 16: STEPS OF THE INDUCTIVE CATEGORY DEVELOPMENT

Within the logic of inductive category development, the theme of categories was previously defined (Mayring, 2014). The following category themes were used throughout the analysis of the text: the drivers of adoption of DLT technology within the scope of capital raising, the classic IPO process and the classic processes of capital raising, the legal issues relevant to the adoption of DLT technologies in the financial field. The level of abstraction refers to the way in which narrow or broad categories are formed. For this thesis, abstraction levels refer to any statement describing the implementation of DLT technologies within the capital raising system. Subsequently, the material was carefully processed and the material that referred to the definition of the category, was formulated into categories. If a passage of text could not be listed in one of the previous categories, a new category emerged until new categories were found. Once all interviews had been processed, the identified categories were reviewed and examined to verify their suitability for the research question.

3.5 VALIDITY AND RELIABILITY

Finally, it was necessary to check and ensure the validity and reliability of the material and the analysis. Qualitative validity describes the accuracy of the material and analysis [34]. Three steps were followed to check the validity following the idea of Creswell and Miller (2000): "Researcher's lens, member checks and peer review". First, the 3 interviewed provided multiple sources of information and the categories identified and conclusions were carefully examined. Secondly, all interviews were sent to the respondents to ensure that everything was understood correctly. In addition, the results and suggestions were shared and examined by the participants. In this way the validity of the information was established. Reliability refers to the idea that the same results would emerge if further research followed the method [33]. In order to achieve reliability, all phases of the research and actions taken were documented as accurately as possible.

4. FINDINGS AND CONCLUSIONS

In this last chapter, the real analysis is conducted on the basis of the comparison among all the different experts' opinions collected through the interviews and the literature review. This chapter will also summarize the modus operandi of the analysis made, the main considerations regarding the comparison of the thesis and the questions posed by the thesis, the findings, conclusions and recommendations on what would facilitate the taking of technology in the future.

4.1 THE ANALYSIS

Once the literature review was completed, as indicated in chapter 3, an exploratory-descriptive research method was used and then experts were interviewed to outline a common opinion and a future vision of what security tokens will be like in the near future (with a time horizon of 5-10 years).

Given the questions posed by the thesis, the ideal interviewee should have had in-depth knowledge about the processes of raising capital and IPOs in particular and at the same time be aware of the potential of blockchain technology and, specifically, of security tokens. Usually, however, the profiles available for the interviews were of professionals experienced in blockchain or experts in the processes of raising capital. Despite this common polarization of knowledge, we tried to always interview subjects who had at least a basic knowledge of both topics even though they were experts in only one of them. The subjects interviewed come from international organizations, investment banks, private equity funds, large consulting firms or with a focus on cybersecurity, financial market and DLT. For the reasons listed above, before each interview we tried to verify and deepen our knowledge about the questions posed by this thesis work.

The interviews, always conducted by four open-ended questions (Appendix A) with a focus on the interaction between Security Token and the processes of raising capital, lasted more or less time but all respondents showed a strong interest in the topic. This is one of the first discoveries of the thesis, which shows that even those who in the short term are less enthusiastic about the interaction between DLT and the processes of raising capital, are aware that in the medium to long term, with the refinement of the technology itself and with the right legal-economic ecosystem, the blockchain can certainly play a key role in the process of listing on the stock exchange.

The following paragraphs summarise the main findings and recommendations implied by the conclusions and by what was discovered in the thesis.

4.2 THE COMPARISON: STOS VS IPOS

Fist of all, to better illustrate the findings and conclusions proposed at the end of this thesis, it's useful to present a brief comparison that shows as an IPO process could be done through security tokens (a process that we called Security Token Offering or, in short, STO). The two processes are compared by the scheme (figure 17) which immediately shows how issuers and investors are put into contact through far fewer intermediaries in the STO process.

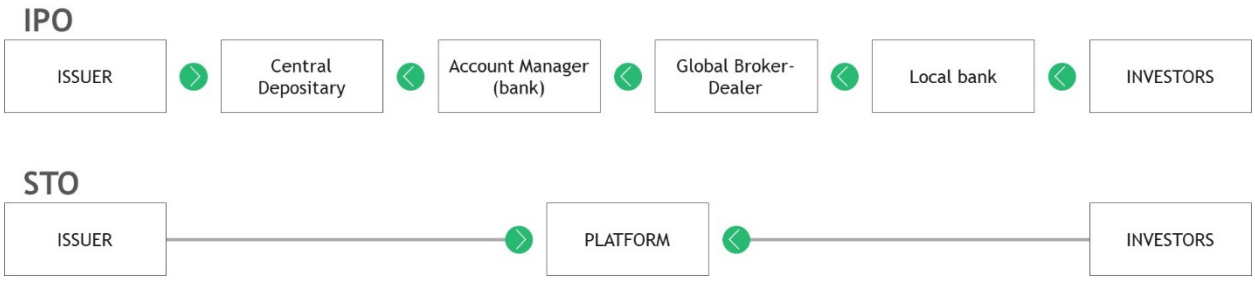

FIGURE 17: IPO PROCESS VS STO PROCESS

Now, returning to the explanation of the parties involved in the current IPO process, considerations about their role in a future STO process are added for each of them. Obviously, it must first be considered that all obligations and responsibilities, however, must be

respected because they are necessary to the intrinsic process of opening up capital to the markets. Obviously, some of them will be obligations and responsibilities 'induced' implicitly by the fact that the company's shares will be present on a public market managed by supply and demand, while others will be more trivially 'imposed' by supervisory bodies to protect investors.

In addition, considering the strategic aspects of listing, some questions come to mind that the company and management should ask themselves before embarking on this path (for example, where is the business plan taking us? what are the actual needs in terms of financing? how strong is the competitive advantage, and how sustainable and developable can it be? how is the quality of management, it needs to be possibly reinforced?). All these questions would have the same exact importance even in the case of STO since, strategically speaking, it is the same thing and that is the opening of corporate capital to the markets.

Below is a hypothesis of the roles of third parties in a possible future STO process:

- **The sponsor**: this is a key figure for the company and will certainly always remain involved in the processes of opening capital to markets. Obviously, it is likely that new types of sponsors will emerge that with the arrival of the STOs will have to be more focused and specialized in digital finance and more agile to move in a new and different environment of investors.
- **Financial advisor**: this too could remain, but it is possible that it is replaced by a general advisor and computerized or in which there is less human involvement (using the AI) that provides the same services, or almost, in a simpler but also more approximate (as already happens for some platform of issuance of security tokens). One has to take into account, however, the great role behind the scenes of the financial advisor who sometimes instructs the customer (the company that wants to put shares on the market) and makes him more aware and ready to change the structure required by an IPO.
- **Independent auditors**: despite the fact that many verifications could be done in a safe and immediate way, these consultants, too, sometimes, contribute to the training of the subject and his preparation to face the market;

- **Law Firm**: the role of the legal advisor depends on the evolution of the regulatory environment regarding the security tokens. If, as mentioned above, all the current legal requirements and adjustments were needed, then it is likely that an advisor specialized in this will be needed. However, the great power of smart contracts must be taken into account, as they could fully replace the role of the legal advisor for the STO process;
- **Communication consultant**: role unchanged since it does not concern the process itself, but has a very powerful impact on it;
- **Tax advisor**: the same reasoning as for legal advisors applies;
- **Supervisors and post-trading services companies**: these are the third parties which are maybe the most impacted since they could be totally replaced thanks to the power of the blockchain technology explained in the previous chapters.

4.3 FINDINGS AND CONCLUSIONS

Finally, the findings and conclusions of this analysis are presented. These are shown under each of the categories identified, as explained in chapter 3 (Methodology) and, in this way, these conclusions will try to respond in a structured way to the questions posed in the introduction. These considerations are the result of the intersection of the thoughts of the experts, perceived during the interviews and research done and analysed in chapter 2 (Literature review). Here are the conclusions (in quotation marks, some of the quotations taken from the interviews made during this research work):

Technical advantages

The post offering administration will be a lot more easy and cheaper with STOs compared to IPOs, this is thanks to the advantages brought from the DLTs technologies. In addition, thanks to this process, it will be possible to cancel the geographical limits currently present for listing on the stock exchange. In this regard, a partner of a major Italian investment bank argues that: "*Certainly, the great advantage from the company's point of view will also be to have access*

to capital from all over the world. With technology, it will be much easier to access investments on stock exchanges on other continents without risk and with fluid and fast processes that can be managed comfortably from a computer or smartphone. Clearly, this is also a great advantage and especially for private investors for whom, until now, it was not easy to access investments in foreign exchanges in a simple way and without any intermediary. The costs of these operations will also be reduced and the verification and KYC processes could become simple and automatic despite the geographical distance." The issued token is not linked to any particular exchange and will not depend on the quarterly expectations of analysts.

The easier and cheaper administration of the offering and post-offering is also due to easier compliance with laws and requirements. Compliance can be enforced by code, all legal requirements can be programmed in the token and the whole process becomes automatic. Other advantages already listed and confirmed by the experts during the interviews are those already listed in the literature review, with particular attention to the best monitoring and safe and immediate management of their actions and cap tables.

Adaptability to the IPO process

Of course, there are many advantages to this, especially in terms of process times and costs, which are extremely low. The increase in speed is due to the coming into play of the technology itself, while the decrease in costs is mainly due to the different and new type of digital stock exchange and the substantial reduction of the parties involved. Here are the words of Raffaele Battaglini: "*The security tokens, being programmable, allow the incorporation of specific rights with the consequent possibility of:*

- *issue shares/units and participative instruments whose patrimonial rights, and their execution, are automated by means of smart contracts*
- *issue shares/units that automate social and shareholders' rights such as pre-emption and multi-sell through smart contracts*
- *and the opportunity to issue flexible instruments/products according to specific market needs, which often have very specific and non-standardised requirements*"

And the some comments from James Bevilacqua: "*What seems to have the greatest impact is the potential to create a more direct link between investors and the shares they own in companies, creating a driving force for social life and participation (the sense of community, as proposed by the ICO model in a way that is often unsuccessful...) and at the same time giving dynamism and simplicity in the purchase and management of shares (which would then be tokenized, with what it entails in terms of value, exchangeability, holding). This is in favour of the issuer and with considerable economic savings, since it will tend to eliminate various intermediate processes and, therefore, related intermediate subjects or intermediaries*."

As Michela Agostini, investment banking associate, who has taken care of and seen closely several IPO processes, said: *"The IPO process is always too dependent on the laws and the structure of the local stock exchange. Only by updating the legislative system and the control bodies and connecting them in a profound way with what technology could do (for example through smart contracts), could we see a real increase in the number of STOs even for the most important brands."*

Finally, the advantage brought to IPO processes by security tokens is certainly not as transformational as it probably could be for the secondary market or for the issuance of capital in private companies. Here, through the system explained in chapter two and as confirmed by the interviewees, the private STOs could provoke a huge unblocking of liquidity in total security and efficiency (through the system of whitelists explained in chapter 2). Here the transformation would be really disruptive and would involve an important change of the world economic ecosystem. Enrico Ferro, professional and expert in the blockchain field, claims that *"DLT will represent a open opportunity for small investors (e.g.: EU investors having access to American & Asian Startups), for entrepreneurs easier access to a global financial market and an lower reliance on gate keepers (VCs)*", confirming that there will be a real value added of the application of DLT to the raising capital process mainly for startups and small medium enterprises and investors.

4.4 FUTURE SCENARIOS AND RECOMMENDATIONS

Common thinking is highly optimistic about the position of security tokens in the financial markets. James Bevilacqua words, perfectly explain the previous line: "*I firmly believe that STOs will become established over the next 4-5 years as an alternative method of managing stock options, offering viable alternatives to current systems and processes. I cannot predict whether there will be a complete "replacement" in ten years because we do not have enough evidence today to make this assessment. In 2017/2018 it was thought that the ICOs would destroy the crowdfunding and bring out the new giants like Google, Facebook, Amazon, in a few months, which has not happened at all, indeed, we are facing the mortality phase, and we are only at the beginning of the curve. This process hasn't even started with STOs yet, so there's a lot to wait and see. Surely in the future, I don't know how close or how remote, tokens will be the only method to mark "the property" and one or more cryptocurrencies will be the only money available. This is a next step in the economic and financial development of mankind*."

In reality, despite the highly optimistic and enthusiastic thoughts of the experts, the future scenarios can be multiple and all different but characterized and united by the strong impact of the legislative system on the security tokens. Partial or total adoption is plausible, but it is still difficult to try to estimate the time when STOs will regularly replace IPOs.

Certainly the blockchain technology will play a fundamental role in the financial field, but for the Security Token Offerings to become so common that they are preferred to the classic IPOs, there is certainly a need for a change in the economic-legislative infrastructure in which these operations take place. This change is already taking place in different ways and at different speeds in the capitals of the blockchain world such as the USA, Switzerland, Malta and Singapore, but also in various European countries and Italy. However, it is always difficult to understand how the legal environment should act in these cases: should the law follow and develop according to the advancement of the technology itself or should it guide and pave the way, anticipating the taking of technology in the processes already used, so that it can be used by all? There are various opinions on the matter, but given the extreme interest of states and

investors, international institutions and organizations are paying close attention to the problem by identifying and forming teams of experts who can help states themselves to anticipate the advancement of the technology by mitigating the risks that this could bring and at the same time facilitating its taking. Given the vision of the experts interviewed and the opinions of the literature on the subject, I think the latter is the most appropriate way to proceed. The main recommendation for the future is to continue to adapt the legal environment to this technology, trying to create a protected environment where the first experiments can give room for errors and improvements regarding the processes of raising and exchanging capital through security tokens. The predictability and complete knowledge of the use of security tokens, already in the possession of experts and experts, should in the coming years only seek confirmation of what is already clear and proceed to make the use of this technology common with an ever faster step.

BIBLIOGRAPHY

[1] Deloitte Insights, «Deloitte's 2019 Blockchain Survey» 2019.

[2] M. Swan, «Blockchain_ Blueprint for a New Economy, 1 a cura di, O'Reilly Media» 2015.

[3] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008.

[4] M. Mainelli e M. Smith, «Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)» 2015.

[5] E. Piscini, M. Cotteeler e J. Holdowsky, «Blockchain: A technical primer,» Deloitte's technology consulting, 2018.

[6] V. Buterin e J. Weissman, «Sharding FAQs,» 2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQs#this-sounds-like-theres-some-kind-of-scalability-trilemma-at-play-what-is-this-trilemma-and-can-we-break-through-it. [Consulted on 17-04-2019].

[7] J. Abadi e M. Brunnermeier, «Blockchain Economics *,» 2018.

[8] L. ABI e B. C. C. Reply, «LE BANCHE E LA BLOCKCHAIN: QUALI OPPORTUNITÀ? RICERCA DI SCENARIO,» 2017.

[9] L. Lamport, R. Shostak e M. Pease, «The Byzantine Generals Problem,» 1982.

[10] P. Andrew, «What is Proof of Capacity? An Eco-Friendly Mining Solution,» 2018. [Online]. Available: https://coincentral.com/what-is-proof-of-capacity/. [Consultato il giorno 01 02 2018].

[11] P. Garg, «What is a coin burn?,» 2018. [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_burn. [Consultato il giorno 02 02 2018].

[12] K. Rilee, «Understanding Hyperledger Sawtooth — Proof of Elapsed Time,» 2018. [Online]. Available: https://medium.com/kokster/understanding-hyperledger-sawtooth-proof-of-elapsed-time-e0c303577ec1. [Consultato il giorno 03 05 2018].

[13] M. Thake, «What is Proof of Stake? (PoS),» 2018. [Online]. Available: https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a. [Consultato il giorno 25 07 2018].

[14] J. Martinez, «Understanding Proof of Stake: The Nothing at Stake Theory,» 2018. [Online]. Available: https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027. [Consultato il giorno 29 06 2018].

[15] G. Konstantopoulos, «Scalability Tradeoffs: Why "The Ethereum Killer" Hasn't Arrived Yet,» 2018. [Online]. Available: https://medium.com/loom-network/scalability-tradeoffs-why-the-ethereum-killer-hasnt-arrived-yet-8f60a88e46c0. [Consultato il giorno 16 05 2018].

[16] «Bitcoin Developer Reference,» [Online]. Available: https://bitcoin.org/en/developer-reference. [Consultato il giorno 12 03 2018].

[17] . . Shermin, . Voshmgir, . . Valentin e . Kalinov, «Blockchain A Beginners Guide,» 2017.

[18] P. Tasca, T. Thanabalasingham e C. J. Tessone, «Ontology of Blockchain Technologies. Principles of Identification and Classification,» 2017.

[19] EBA, «Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios An exploration for transaction banking and payments professionals EBA Working Group on Electronic and Alternative Payments,» 2015.

[20] J. Song, «The Truth about Smart Contracts,» 2018. [Online]. Available: https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f. [Consultato il giorno 25 06 2018].

[21] I. Nikolic, A. Kolluri, P. Saxena e A. Hobor, «Finding The Greedy, Prodigal, and Suicidal Contracts at Scale,» 2018.

[22] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda e V. Santamaria, «Blockchain and smart contract for insurance: is the technology mature enough?,» Future internet, 2018.

[23] M. Cantamessa e F. Montagna, «Management of innovation and product development,» 2016.

[24] Dr. Gavin Wood, «Ethereum: a secure decentralized generalized transaction ledger» 2014.

[25] Vitalik Buterin, «Ethereum White Paper - A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM» 2013.

[26] Ritesh Modi, «https://medium.com/coinmonks/https-medium-com-ritesh-modi-solidity-chapter1-63dfaff08a11» 2018.

[27] Ben Edgington, «https://notes.ethereum.org/c/Sk8Zs--CQ/https%3A%2F%2Fbenjaminion.xyz%2Fnewineth2%2F20190329.html» 2019.

[28] James J. Park, «When are tokens securities? Some Questions from the perplexed» 2018.

[29] Mayring, P., «Qualitative content analysis: theoretical foundation, basic procedures and software solution. Klagenfurt» 2014.

[30] John W. Creswell, «Research Design: Qualitative, Quantitative, and Mixed Methods Approaches» 2009.

[31] Eisenhardt and Graebner, «THEORY BUILDING FROM CASES: OPPORTUNITIES AND CHALLENGES» 2007.

[32] Alexander Bogner, Beate Littig & Wolfgang Menz, «Das Experteninterview. Theorie, Methode, Anwendung [The Expert Interview: Theory, Method and Application]» 2002.

[33] Yin, R.K. «Case Study Research. Thousands Oaks: SAGE» 2008.

[34] John W. Creswell and Dana L. Miller, «Determining Validity in Qualitative Inquiry» 2000.

[35] Clay Collins, podcast «Flippening – Tokenize The World: A Security Token Documentary» 2018.

[36] Clay Collins, podcast «Flippening – Tokenize The World, Part 2: A Security Token Documentary» 2018.

[37] Clay Collins, podcast «Flippening – Tokenize The World, Part 3: A Security Token Documentary» 2018.

[38] Politecnico di Milano, Intermonte sim «Quaderno di ricerca Intermonte - L'IPO come mezzo per finanziare la crescita: raccolta di capitale e utilizzo dei proceeds» 2017.

[39] «Cambridge Judge Business School: Cambridge Centre for Alternative Finance», 2015.

[40] M. Del Barba, «Il crowdfunding supera i fondi di VC. Così cresce la finanza alternativa», Il Corriere della Sera, 2017.

[41] R. De Luca, «Il crowdfunding: quadro normativo, aspetti operativi e opportunità», Fondazione Nazionale dei Commercialisti, 2015.

[42] A. Delivorias, «Crowdfunding in Europe. Introduction and state of play», European Parliamentary Research Service (ERPS), 2017.

[43] P. Pais, C. Perretti, Spinelli, «Crowdfunding. La via collaborativa all'imprenditorialità», 2014

[44] «Report italiano sul CrowdInvesting», Politecnico di Milano - School of Management, 2017.

[45] «Initial Coin Offerings (ICOs) for SME Financing», OECD, 2019.

[46] S. Alineri, P. Pia, «Ipo: un'analisi delle dinamiche interne e del ruolo dei soggetti coinvolti», 2002

[47] S. Frisina, B. Matarazzo, «Modelli teorici e analisi empiriche sulle Ipo: il caso italiano», 2000

[48] S. Ricco, «La quotazione in borsa: costo o investimento?», 2017

[49] «Quotarsi in Borsa, Borsa Italiana S.p.A.», 2001

Websites articles:

How Tokenization can Unlock a Multi-Billion Dollar Liquidity Premium Market - https://medium.com/lendflo/how-tokenization-can-unlock-a-multi-billion-dollar-liquidity-premium-market-3b167715a3a2

Why Tokenizing Assets is Changing the Finance Industry - https://medium.com/lendflo/why-tokenizing-assets-is-changing-the-finance-industry-8890588540db

Imprese e blockchain, quattro strategie e un problema: l'Italia - https://www.econopoly.ilsole24ore.com/2019/01/22/imprese-blockchain-strategie-italia/

Da bitcoin a tokenizzazione: manuale rapido per capire (e usare) la blockchain - https://www.econopoly.ilsole24ore.com/2018/11/13/bitcoin-tokenizzazione-blockchain/

Perché la rivoluzione tech più importante del secolo non è uno schema Ponzi - https://www.econopoly.ilsole24ore.com/2018/09/12/blockchain-rivoluzione-schema-ponzi/

Blockchain e Governance: gli ambiti applicativi nell'Impresa 4.0 con le DLT - https://www.blockchain4innovation.it/mercati/industria4-0/blockchain-governance-gli-ambiti-applicativi-nellimpresa-4-0-le-dlt/

The "Tokenomics" of an Equity Token - https://medium.com/@ph3nomaly/the-tokenomics-of-an-equity-token-71a67a2fdd06

SECURITIES DIRECTIVES IN EU - https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en

APPENDIX A

Scheme for interviews: four main questions around which discussions were created about the topic presented by this thesis.

1. How do you think DLT technologies will revolutionize the capital markets and, in particular, the ways of raising capital currently used by public and private companies?
2. How do you think security tokens will impact the IPO process? Which parts of the process will be more affected by the introduction of the new technology and why?
3. Do you think the current legal environment (in your geographical area of competence) is ready to support the introduction of security tokens? Which are the main improvements you would suggest to make the legal landscape ready to support the introduction of security tokens?
4. What is your view of security tokens future (next 10 years)?