Ca' Foscari
University
of Venice

Master's Degree Programme

Economia e Gestione delle Aziende

Curriculum "International Management"
Second Cycle (D.M. 270/2004)

Final Thesis

The Evolution of Equity Crowdfunding Through Blockchain Technology: The Bloomio case

Supervisor
Ch. Prof. Giovanni Vaia

Graduand
Giovanni Avogadro
Matriculation Number 844580

Academic Year
2016 / 2017

- This page has been intentionally left blank -

Thanks to

I had the chance to work, but most importantly become friends, with some of the most interesting and capable individuals I've ever met; during the curse of this unforgettable university experience. They have changed me profoundly, and helped me to grow into a new and better professional and individual. I owe a lot to them, and I am extremely thankful.

My gratitude goes especially to my family, that taught me the importance of education and the meaning of learning.

Abstract

The new concepts brought up by the introduction of Blockchain technology are changing many industries at once, with the promise of democratization and of the increase in transparency of company infrastructure and of operations. The equity crowdfunding industry is one of the industries that could be radically transformed by the introduction of the technology.

Through this thesis, we will present an introduction to the concepts behind blockchain technology, and equity crowdfunding. We will then analyse the limitations that the current methodologies and services associated with equity crowdfunding might present, and how the introduction of the technology might mitigate these inefficiencies.

We will finally analyse the case of Bloomio; a Swiss-based equity crowdfunding company, which is the first one in the world to have implemented blockchain technology in its operations.

Table of Content

Introduction

The invention of the Database by IBM in 1970, revolutionized the world; so much that right now, every aspect of our society depends on this idea of recovering and storing information.

Blockchain is now about to revolutionize databases, which will in turn revolutionize again every aspect of our society.

Blockchain is about creating a "database" which is accessible by anyone or anything at any time, working like a network instead of having a single point of failure. The secret is Decentralization.

Decentralization offers the chance to individuals to interact and cooperate with each other, without the need of a central authority or a middleman.

This new technology is influencing step by step many industries, and the promise of a democratization of the world is increasing its notoriety by the minute.

Whenever the middleman is eliminated, efficiency rises substantially. The need to scale in order to satisfy the huge supply chains we have created, makes us rely on deals made on humongous quantities. Blockchain and its decentralized system would change that, and would help small business to compete with the industry giants.

The technology is still new and not everyone has a complete grasp of its functionalities, potential and future development. Even though the technology is almost 10 years old, we are just seeing now the first attempts to transform it in something valuable for companies but most importantly for people.

As it frequently happens, regulators are being sceptical and slow in the determination of the legal boundaries of the technology, but this is not scaring industry giants and innovation enthusiasts in the exploration of it.

Many industries are changing to adapt to this innovation, but the first industry to be affected is of curse the financial one. Given the nature of the technology, the crowdfunding industry is also changing rather rapidly; it is acceptable to believe, that this ecosystem and the world economy, will undergo extreme changes in the next few years.

CHAPTER I

Blockchain Technology, a Focus on The Ethereum Network

"Saying that blockchain is a new form of database, is like saying that e-mail is a new way to send people letters"

Bill Gates, 2017

Blockchain is a public, trusted and shared ledger (The Economist, 2017). Shared since it is based on peer-to-peer network, meaning that it is not controlled or managed by a single individual, but by all its participants. It is available to all, hence public; and data cannot be manipulated without being approved by everyone in the network, which makes it a trusted ledger. This specific set of attributes, make the Blockchain technology not only more secure when managing sensible data, but also able to eliminate intermediaries when transferring information in a decentralized manner.

Blockchain technology is usually associated with the virtual cryptocurrency "Bitcoin" but the potential of it is not necessarily associated with currency transactions. Blockchain can be adapted to fit many industries and business models, but most importantly, it can be used to create organizations able to support themselves in a complete decentralized matter.

The Blockchain has been of interest for many people since it came out in 2009. It is part of the 4th industrial revolution characterized by a fusion of technologies that is blurring the lines between the physical, digital and biological sphere (Schwab, 2017), full of disruption and disruptors, and together with many others has the potential to impact heavily on society.

Blockchain can be defined as a "distributed database or ledger", which uses a secure protocol where a network of servers, also called "Nodes", collectively verifies a transaction before it can be recorded and approved. Therefore, blockchains can be used to create trust, not reliable on a third party anymore, but on the technology itself; by enabling people who do not know each other (and thus have no underlying basis for trust)

to collaborate without going through a central authority (Schwab, 2017). It is a shared database controlled by the network with no individual party exercising central control.
In non-technical terms, a blockchain can be seen as a large and transparent spread shit, where all transaction or assets of an organization are chronologically and permanently stored since the creation of that entity. All the transactions are also maintained and verified by all peers in a decentralized way, making it extremely transparent and globally recognized as true.
To better understand this technology and its process, we want to go deeper in the description of all the most important characteristics and terms associated with this new technology.

1.1. Trust

Two precondition of trust are risk and interdependence (Chen & Dhillon, 2003). There has to be in fact interdependence between the trustee and trustor. If that's not the case, no matter how intricate their actions are, they do not effect one another. Moreover, if there is no uncertainty, no action by the trustee can change the events, and thus, no trust is needed. Trust can also be defined as a two-sided, asymmetric relationship between entities; the trustee or recipient of the trust can be anything, from a person, an object, a process or a computer algorithm. Sometimes though, the trust relationship has to be constructed from both sides of the relationship. Trust has also a scope and can be contingent to specific circumstances; that defines under which rules or occasions we may want to trust someone or something, and what actions we trust them to perform on our behalf.
In the economic exchange world, we can find three different types of trust: institutions-based, characteristic-based, process-based.

Institution-based trust:
Institution-based Trust comes from an authority that is centralized. This is the example of a commercial bank, that we trust to manage our money as a centralized institution.

Characteristic-based trust:
Characteristic-based trust is the trust we have in some people because of the similarities between ours and their characteristics, taste, origin, or even values in life. We tend to trust

more people with a similar background, and that share similar perception of the world to ours.

Process-based trust:
Process-based trust is rooted into social micro-rules and norms, according to which when facing a known interaction with someone, we are able to theoretically predict the response by the counterpart. For example, we expect someone to answer when asked a question.

Consequently, given the differences in the type of trust, there are also differences in the type of trust fail depending on the type of trust we are facing. Trust can be lost if a central organization fails, if the person you trust fails, or if the the process you trust fails.
On-line trust assumes an even more important role, since:

"The degree of uncertainty, dependency, and risk is higher in the on-line world than in the off-line world"

Zainab M. Aljazzaf, 2010

Uncertainty and dependency assume an even stronger role in the on-line world, where traditional techniques to hold trust do not hold any more and trustworthy relationships are created around a reputation system.
In using Blockchain technology, people may find it hard to trust the process or a computer program, but some of them are drown to trust the technology when friends or people that share a similar vision and interact in the same sphere become early adopter of the technology. Note that the types of trust involved in this type of relationship are characteristic-based and process-based trust, that compose the mix of trust relationship that evolve around blockchain technology.
We need to remember that is not the technology itself that defines what is really true, and it could occur the case in which not everything that is on the blockchain is true. What the blockchain does in fact, is verify that a certain data was inputted in the system at a specific moment in time and store that information for ever, but it cannot guarantee that that piece of information is necessarily true. The ones that define if that information is true or not, are the users inside the network, that validate the transaction.

Blockchain affects trust in several ways in the business context. The protocol layer and the business layer of the blockchain, both affect trust and its perception in the system. In the protocol layer we can have two major benefits, namely transparency and security. These two characteristics are made possible by the technology, through the use of its system of immutable history of transactions and the use of public and private keys[1]. Security can also be increased by decentralization and encryption, making the system more private and safer. Security and transparency can be considered some of the most important characteristic of this technology, that directly influence trust.
In the business layer instead, trust is affected by the creation of rules, rights and restriction to user's actions, that can be implemented in the code of the programs that regulate the transactions called smart contracts[2], that can improve trust or even make it pointless.

1.2. Digital Signature

The digital signature scheme, invented by Whitfield Diffie and Marti Hellman, explained in their seminal paper: "New Directions in Cryptography", is the digital correspondent of a paper signature used in the blockchain transaction system. Through it, every user is allowed to have one or more "public key" and "private key".
A public key is a publicly available key, in the form of a string of bits. It is like a bank account number, anyone can see it, and it is associated with one person in particular; it is than a traceable and transparent way to identify a person. The private key on the other hand, is still a string of bits, but it is only available and visible, to the single user, it can be defined as a digital ID than only the user holds, and no one else can. It is a digital and unique identification for an individual or a machine.

Public and private key can be used in the validation of a transaction, in which both parties involved agree on the execution. The transaction can be a transfer of currency, property, data, or a simple communication or the expression of a right; this entitles the users to determine whether they want to be involved in that transaction or not.
This system was created to allow for a high level of security and transparency and to make sure that both parties in the transaction are protected and aware of the transaction. The process of validation of a transaction can be summarized as such:

[1] Section: 1.2 Digital Signature.
[2] Section: 1.5.3 Smart Contracts.

1) The transaction is broadcasted by the sender to the nodes in the network. Each transaction is protected by a "digital signature". Transactions are sent to the public key of the receiver using the private key of the sender. By using a precise private key, the sender is proving the ownership of that private key linked to his identity. The receiver of the transaction verifies the digital signature on the transaction through the use of his own private key proving his identity and demonstrating that he accepted the transaction and is aware of it.
2) Once it is accepted by the parties involved, the transaction is sent to all the nodes in the blockchain, that check it and approve it making sure that all the conditions inside the transaction are met to be recorded permanently in the system. Consensus[3] between the nodes inside the network is necessary for the validation and transcription of the transaction in the public ledger.

We will take a closer look at the concept of "Consensus" in section 1.4, but for the sake of clarity, we can say that consensus means that before recording any transactions in the public ledger, verifying nodes[4] have to agree on the truthfulness and feasibility of the proposed transactions before recording it in the ledger. One of the conditions for the transaction to be feasible for example, is to ensure that the spender own the right amount of currency; hence that he has sufficient funds to support the transaction. Even more important condition for the system to certify a transaction, is the presence and the validation of both the signatures of the parties involved.

The use of signatures is not limited to commerce transactions, but can be used for every form of official transaction, in fact with this system, all sorts of transactions and transfer of ownership can be carried out digitally. Digital and paper based signatures have two important characteristics in common; they both guarantee that a defined piece of information passed from one site to another without being altered; and they can both allow the receiver to prove to a third party that he received that piece of information directly form the signer. The main difference lies in the fact that the traditional methods, rely on the certification of the transaction by a trusted third party like a bank, a layer or a notary; in the case of the blockchain on the other hand, transaction validation is performed by the network, in a decentralized, transparent and secure way. Furthermore,

[3] Section: 1.4 Consensus and Mining.
[4] **Verifying Nodes:** Nodes in the network devoted specifically to the validation of transactions.

information about all transactions and interactions, are secure and not guarded by a single individual but by the whole system in a decentralized matter. We would like to inform the reader, that the similarities to the traditional system of certification of transactions, led to the certification by the united states of Digital Signatures as legally binding[5].

1.3. Hashes and the Sequence of Transactions

The Blockchain construction is composed by "blocks" containing all transactions; this means that every transaction ever made on the platform is stored in groups of transactions that have happened at the same time. These blocks are linked to each other inside the blockchain, creating a chronological order of transactions that are secure, immutable, and untouchable.

Having this concept in mind, the chance might be that one or more untrustworthy nodes will make parallel transactions, sending the same amount to two different recipients. This act is called double-spending, and a mechanism is established to avoid it from happening. The mechanism that prevent these situations from happening is called mining; based on the proof-of-work (PoW) scheme that we will discuss in the next section. Before we go into detail with mining and PoW, we want to explain what defines the chronological order between the blocks in the blockchain.

To ensure that all blocks follow each other in the defined order, each block is given a "hash" that will determine the order of the block inside the chain.

The first block is called the genesis block, and each block that followed contains the hash of the previous block. The chain of hashes, constitutes the "chain" in blockchain.

1.4. Consensus and Mining

The use of consensus is necessary for many functions both economic and social. There are benefits and empowerment for everyone trusting a single ledger, starting from a faster way to reach a settlement, or the elimination of fraudulent actions. Traditionally, consensus is given by a central authority like the government, notary agency and so on, but the traditional system is expensive, labour-intensive and centralized. What the blockchain technology aims at, is creating a consensus system that is cheaper, democratic and less risky. This is done by making consensus decentralized, making it more secure,

[5] http://usinfo.state.gov/opical/global/ecom/00063001.htm

and creating rewards for maintaining it cost effective; improving processing power, without incurring in too much social costs.

Consensus means that nodes agree on the same state[6] all the time (Henning Diedrich, 2017), and the order in which the blocks of the blockchain should be put. All the nodes in charge of consensus, need to agree on the truth of transactions and on the order of the blocks that compose the blockchain

The ones that need to achieve consensus are the so called "miners", and they are the nodes that decide to take part to the consensus building mechanism. Through this mechanism, valid transactions are selected by the network to compose a block which miners than validate in order to make it able to attach it to the next available spot in the blockchain.

1.4.1. The Mining Process

We will now try to give a more in depth definition of mining and explain why it is so important for the creation of the chain.

Mining is the process through which transactions are verified and once verified, stored inside the public ledger (Sterry, D. R., 2012), and the method for the extraction and release of cryptocurrency.

The mining process consists in the aggregation of transactions into a block, and use the computing power at the disposal of the miner, to find the solution to a mathematical problem. The result of such a mathematical problem will be the right hash, meaning the hash that is consequent to the hash of the last block attached to the blockchain.

Miners need to win the mining process (the race to find the right hash) to be the first one to attach the new block to the blockchain. Whoever wins the mining process, will be allowed to broadcast the new block to the rest of the network updating the chain; this way, only real and approved blocks can be put on the chain, avoiding the creation of malicious blocks with false information. The winner of the mining race, is also reworded with cryptocurrency; this process allows for the distribution of new coins in the system, and at the same time provides an incentive for nodes to participate to the mining process. Without this incentive, the mining process would be too expensive in terms of energy consumption, to push nodes to mine transactions.

The mining process for the finding of the right hash, usually takes 10 minutes. With the increasing of the velocity with which mines are able to find hashes, the mathematical

[6] **State:** is the totality of the data and the transactions that have been written on the blockchain since the genesis block.

problems to be solved become harder, in order to maintain the hash finding process around ten minutes.

1.4.2. Nakamoto Consensus

The consensus protocol of Bitcoin is also called the "Nakamoto consensus", named after the creator of Bitcoins Satoshi Nakamoto (Nakamoto S., 2008). Nakamoto consensus can be defined with a sentence as: "the longest chain wins". To understand this definition, we first explain the concept of a fork.

As we know, consensus refers to the situation in which all miners agree on the right spot in which a new block should be put, depending on the hash that the block is associated with. There is the remote possibility though, in which two miners will find the solution to the mathematical problem - and hence the right hash - at the same time. In these situations, the chain splits and created what is commonly known as a "fork", which can be resolved through different methods depending on the nature of the ledger. In the case of the Bitcoin ledger, miners keep mining on both branches of the fork, but will try to attach their new blocks only to the branch of the fork that has the most blocks attached to it. After a certain number of blocks are mined, the branch with the most number of blocks attached to it wins, and the other branch is eliminated. This does not result in an elimination of transactions, since the blocks that are eliminated, are exactly the same of the ones that are present on the winning branch.

1.4.3. Permissionless and Permissioned Consensus

There are differences in the modalities of participation to consensus by nodes, depending on the type of ledger that is being created. Participation to the consensus can be permissionless and permissioned; this difference affects deeply the reaching of consensus.

In a permissionless ledger, everyone contributes to consensus. A public blockchain such as "Ethereum"[7], is constructed as such. In a Public blockchain, all participants have to reach consensus over every change to the data. This means that every transaction has to be approved by every peer, even if they do not participate directly to the transaction itself.

[7] **Ethereum:** is an open-source, public, blockchain-based distributed computing platform featuring scripting functionality. It provides a decentralized Turing-complete virtual machine, the **Ethereum** Virtual Machine (EVM), which can execute scripts using an international network of public nodes.

All peers have agreed upon a common ledger and they all have access to all transactions ever recorded.
This system raises some privacy issues even though information is encrypted, together with the effect on performance on transaction processing. The requirement of having every member agree on the state of the ledger takes time to achieve, and it also requires a fair amount of energy.
In a permissioned ledger, to the contrary, consensus power is given to a previously selected number of nodes, only the ones that are directly involved in the transaction. With this system there is a strong control over the circulation of information, resulting in a higher degree of privacy. Furthermore, with having just a limited number of peers obligated to reach consensus, the process results faster and more efficient. Consensus definition here is broad and considers the whole transaction flow. This system requires for different roles to be given to nodes when reaching consensus, differently form a permissionless system, where peers have identical roles.
Each permissioned ledger has its own way to validate transactions, depending on the role that is been given to the single peer.
Within "Fabric" for example, another type of ledger, we have clients, peers, orderers and endorsers, that respectively invoke transactions, maintain the ledger, order updates to the ledger to record new transactions, and check if new transactions fulfil certain sufficient conditions to be put in the ledger.
Another blockchain system, called "Corda", uses a different system, where consensus is determined by validity and uniqueness. Specifically developed software associated with the transaction take care of validity, whether uniqueness makes sure that the transaction in question is the unique consumer of all its input state (Sanders, P. 2017). Notary nodes, on the other hand, reach consensus over uniqueness with a pluggable algorithm.

Blockchain is a way for information to be recorded and shared by a community (Deloitte University Press, 2016), a community in which every member has a copy of the information and all members must validate any change collectively. The information can be anything that can be described digitally like transactions. Information in a public blockchain are transparent, permanent and searchable meaning that each member of the community is able to view all of it. Every update creates a new "Block" that composes the "Chain". New entries to the chain are managed by a protocol that decides how they are initiated, validated, recorded and in the end distributed, and sets the differences that

characterize the different ledgers.

1.5. Ethereum

The blockchain technology can be implemented in many different ways, and research on the field have created different ways to exploit it, creating different types of DLT[8] with different purposes and construction. At the moment three of the most developed DLTs are "Hyperledge Fabric[9]" (Fabric), "R3 Corda[10]" (Corda), and "Ethereum"[11]. These DLT have different visions of the application of blockchain, especially because of the differences in the respective field of work.

Developers from Fabric and Corda focus on specific applications and concrete use cases (Sandner, 2017); Fabric focusses on creating a modular and extendable architecture employable in various industries, focusing on banking and health care, over to supply chain; whereas Corda focuses on the financial service industry.

Ethereum on the other hand presents itself more independent than Fabric of every specific field of application. What stands out for Ethereum is not it's modularity, but the goal of creating a generic platform for all kind of transaction and functions.

Ethereum is a highly flexible DLT with its own currency, that with its powerful smart contracts is capable to make it applicable to any kind of application. The permissionless system and the total transparency although, leads to performance scalability and privacy issues.

Ethereum has a more generic application, and it's very flexible internal software, can have many applications and the capability of creating a "world computer". Ethereum and Bitcoin are both peer-to-peer networks, and share many characteristics, but some concepts and implementations differ from one another. These differences however, make it possible for Ethereum to support and program digital contracts defined by complex logic. For these reasons we will focus our attention on this specific DTL, that together with the related DApp (Decentralized Applications) and DAOs (Decentralized Autonomous Organizations) is changing and will change drastically the way we do business and how we handle sensible information and transactions.

[8] **DLT:** Distributed Ledger Technology.
[9] https://hyperledger-fabric.readthedocs.io/en/release/
[10] https://www.corda.net/
[11] https://www.ethereum.org/

1.5.1. Accounts

Accounts is the system used by Ethereum to represent ownership of value. Any entity that holds a state inside the system in fact, is associated with an account, that has its own private and public key. The private key is the digital ID of the owner of the account, and is needed to sign transactions, certifying the identity of those who sign; the public key on the other hand is the address of the account, which is public and works as the address of the account.

Account objects are composed by four different fields with specific values. Depending on the type of account, the values for these fields change resulting in different properties (Wood G., 2014). These properties are: "Nonce", a counter of the transactions and contracts that went through the account; "Balance", the value retained by the account; "storageRoot", the root hash of the "MarklePatrishaTree[12]", constituting the storage of the account; and the "codeHash", a hash of the code that shows how the account works.

Accounts are than divided into externally owned accounts (EOAs), and Contract Accounts. Externally owned accounts are controlled by a private key and are personal, allowing for interaction between private users like exchange of currency and messages. A Contract Account on the other hand, is a computer program, which is composed by code that holds the logic that controls it (Ethereum frontier guide, 2016).

A Contract Account functions as a deposit account to store value while transactions are taking place on the platform, and can have different functions depending on the information and the code stored inside it. We can think of an example of Contract account if we consider User-A, which wants to buy goods from User-B, but both do not trust each other during the transaction. User-A is able to put the money in a previously constructed Contract Account and wait for the goods to arrive. Once the goods have arrived, both parties will send another message to the contract, that will send the money to User-B. Until both parties approve of the transaction, the money will be locked inside the Contract Account. In order to avoid malicious actions by User-A that would not release the money even after receiving the goods, the agreement could be constructed such that a trusted third party will be involved to settle the dispute.

[12] **Markle Patrisha Tree:** a cryptographic data structure used to store all keys.

1.5.2. Transactions and Messages

Inside Ethereum there is a distinction between what can be considered a transaction and what can be considered a Message. This distinction exists because of the two different types of accounts present in the network.

Peers inside the blockchain, transfer value through transactions. These transactions are generated singularly and then distributed to the rest of the peer-to-peer network.

In order to avoid malicious actions from other nodes in the system, all transactions must be signed by generating account through the use of their own private key; this will authorize the transition by the node that generated the transaction.

Transactions in order to be called as such must contain all the information necessary in order to make that transaction unique and recognizable by the network; this means that they must contain: the total number of transactions sent from the senders account (nonce), the price per computational step (gasPrice[13]), the maximum price for the computation of the transaction (gasLimit[14]), the recipient address (to), the amount to be transferred (value), the signature of both parties (v,r,s), and specify if the transaction will create a new account or will refer to an already existing account (Data/Int) (Wood G., 2014).

Messages on the other hand differ from transactions in the sense that they are communications generated by the execution of transactions. Messages arrive from the transaction that generated a contract. Massages are not needed to be signed because they are never broadcasted to the network, but they are just part of the systems execution environment as the result of the execution of a code. Figure (1), shows how messages and transactions interface with EOAs and contract accounts. As we can see, the external owned account is the origin of all transactions; messages on the other hand are generated from contract accounts to the outside, and in between contract accounts; after been triggered by transactions in the contract account.

[13] Section 1.5.8 Gas.
[14] Section 1.5.8 Gas.

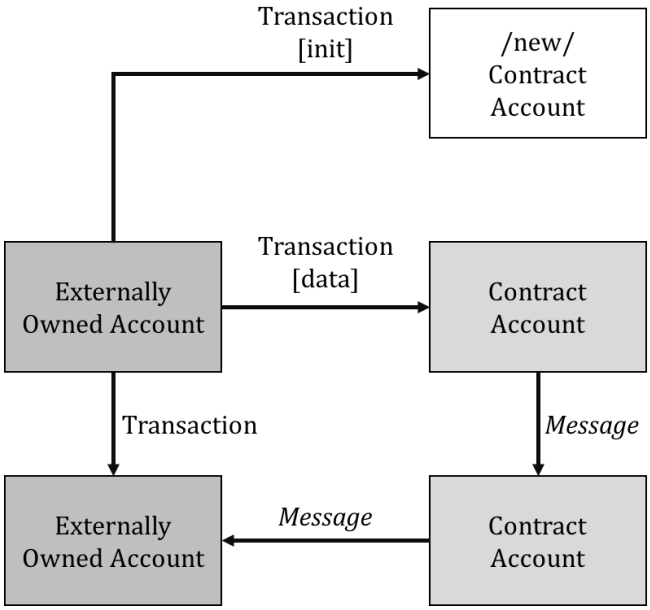


Figure (1): Message and transactions interactions scheme.

Messages have a specific structure composed by elements that carry important information necessary for the functioning of the process. Messages need to contain a sender, the address of the contract that started the message; a transaction originator, the address of the EOA that called the sender contract code execution; a recipient, the address of the beneficiary of the message; the code account to be executed, the account whose code should be carried out, usually a copy of the recipient code; startGas, gas available for the origination of the message; value, the value to be transferred through the message; gasPrice, the price necessary for the computational steps; data, optional data needed for the message; depth of execution stack, the extent of the execution load. (Wood G., 2014)

1.5.3. Smart Contracts

Smart contracts were invented by Nick Szabo in 1994, and required a central authority in his vision in order to function. With the introduction of blockchain, they found another system where they could be implemented.

What characterises Ethereum in fact, is the presence of the so called “Smart Contracts”. A smart contract can be defined as an agreement whose execution is automated (Szabo N., 1994), or as they have been defined more recently:

"A computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs."

(Tapscott D., Tapscott A., 2016)

Such agreement is concluded between two actors as in a peer-to-peer, peer-to-organization or person-to-machine interaction. As soon as certain conditions are met, the contract will be executed and assets, ownership, or currency can be exchanged between the two parties. The transaction resulting, is validated by the members of the network; and thought the methods we previously analysed, stored inside the blockchain.

According to Nick Szabo, smart contracts in order to be defined as such, need to have the following characteristics: visibility, on-line enforceability, verifiability and privity. Visibility means that each participant to the contract should be able to see everyone's compliance to the contract and performance with respect to the terms of the contract; this means that they must also be able to prove to a third party their fulfilment to the terms of the contract.

On-line enforceability refers to the prof of the fulfilment of all the terms in the contract. In order to fulfil this task, measures can be taken than can be divided in proactive and reactive measures. Proactive measures make it impossible to crack terms, while reactive ones block malicious behaviour.

Verifiability refers to the possibility to verify the existence and the validity by external third parties. Verifiability of contracts is necessary for conflict resolution.

Lastly, smart contracts should be private, meaning that the content and conditions of the contract should be available only to the parties involved.

The use of the smart contract, enables the transfer of assets and the execution of transactions without a third party being necessarily aware and involved. These virtual agreements could allow for the creation of a system in which intermediaries are completely eliminated and transactions are carried out without the intervention of a trusted third party.

Smart contracts are simply software written in a programming language. Difference though exist between different blockchains in the role that these codes have. In some networks, these contracts are not just made by code, but may also contain legal prose.

Ethereum have a simpler construction for smart contracts and do not have this feature.
These contracts can be seen as a binding agreement that can move information and money, based on the agreements defined in them. They are unstoppable, guaranteed to resolve themselves, depending on the blockchain and not by a legal system, and easier to read than a legal text that could be falsely interpreted.

Ethereum runs a general blockchain, but it has embodied inside it, a system or machine called Ethereum Virtual Machine (EVM)[15], which it has been created specifically to run and manage these smart contracts. The presence of the Ethereum Virtual Machine is what distinguished - at first - Ethereum from the rest of the blockchain-based platforms.
These smart contracts are written in Solidity, which is a programming language similar to JavaScript[16]. Solidity is now used by different systems that allow for the use of such contracts, since many developers understood the potential of smart contracts and are implementing them, with certain variations, to their version of the blockchain. When the contract is complete, it is linked to the EVM and deployed to an Ethereum address, initiating the relation.
Since smart contracts are deployed to the blockchain, were all the information related to it are accessible to all users, there are a few rules that these contracts must follow to ensure a certain level of security; these characteristics are (Bergquist J. H., 2017):

Damage control:
There should be limitations to the value to be put on a smart contract. If in fact, in the case of the presence of a bug in the contract on which the value is stored, a malfunction in the contract might cause a permanent locking down of that value inside the contracts; without any possibility or reach for it by anyone.

Modularity:
Smart contracts should be as simple and as short as possible, in order to keep readability and avoid misunderstanding by users. Contracts can be interconnected with one another, allowing for the modularization of more complicated transactions. As modularity increases, the system itself improves.

[15] Section: 1.5.6. Ethereum Virtual Machine (EVM).
[16] **Java Script**: Programming language commonly used in web development.

Checks-Effects Functions:
These contracts should be able to check if some preconditions are reached as the first step of the algorithm. If the preconditions are met, the contract can move to the second step, which is able to apply changes to the state-variable. Once these steps are fulfilled, the transaction can take place.

In order to be embodied in the contracts, elements like rights, responsibilities, or allocation of property should have the structure to be translated into code, and allow for an automated achievement of results.
Traditional solutions to this problem - like the use of a third trusted party - involve a high level of human interaction, hence higher managerial costs and risk. With a decentralized system, there is the elimination of the possible creation of monopolistic power exercised by consensus centralized authorities. These facts allow for a different definition of smart contracts as:

"Smart contracts are digital contracts allowing terms contingent on decentralized consensus and are self-enforcing and tamper-proof through automated execution".

(Cong L.W., He Z., 2016)

This definition can be associated, and is consistent with, common definitions used in the legal world (Lauslahti, Mattila, Seppala, et al., 2016), and by Szabo (1998).
As we realized so far, the decentralized technology offered by blockchain enables the use of smart contracts and allows for a greater contractibility and enforcement of agreements, facilitating the exchange of currency, property and anything of value, through the use of automated algorithms and avoiding conflicts.
Inside the Ethereum blockchain, the system uses cryptocurrency to make smart-contracts function, this way there is the almost total elimination of a trusted third party necessity. Ethereum in fact, has its own built in currency called "Ether". This cryptocurrency is used to reward miners but also to pay fees whenever a transaction or a smart contract is executed.

Defining smart contracts to a t is still complicated given the nature of the phenomenon and the relative young age of it. What we know though, is that its core notion is to create contracts on possible events based on a decentralized consensus; with low costs, and with

mathematical and algorithmic execution. In order to support these contracts, we need a distributed ledger with self-executing capabilities like the blockchain.

1.5.4. Smart Identity

In section 1.2 we talked about digital signatures and the concept of private and public key. One of the possible implication of the introduction of these applications, is the creation of the so called Smart Identity or Digital Identity.

In the traditional sense, identity refers to the set of information and characteristics that distinguish one individual from the others. In the cyber world on the other hand, identity of an individual, consists of the digital record associated with him/her. These records are formatted in a standardized way, so that they could be utilized to provide identity information and be used in a standardized way in the deployment of transactions. The construction and standardization of these digital documents, supported by the blockchain, has a list of positive attributes such as: existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection, together with the implementation and support of SSI[17].

Users are enabled trough the blockchain to manage and control their own data independently and not by utilizing a trusted external third party; and at the same time prove their identity when performing any type of interaction with other users in the system.

The process of identity verification on a blockchain-based system, requires what is usually referred to as the "handshake mechanism" (Kikitamara S., 2017). The mechanism is composed by a process divided in three separate actions that, in that sequence, allow for a proper identification of users. "Login", "Verify-Request", and "Create Response" are the three steps of this mechanism and in accordance to these, some applications based on blockchain technology have been developed to manage authentication systems.

Digital identity is necessary and decisive in securing information; it allows for the creation of access mechanism, and allows users to have a personalized and accountable presence on-line, limiting the threat of identity theft. This system also allows for the reduction of unauthorised access to personal information, and data infringement.

[17] **Standing Settlement Instruction**: are instructions to follow, every time a trade is made, usually associated with the transfer of funds and / or securities.

1.5.5. Smart Property

The definition of smart property can be summarized as the capability of a property to be by itself, part of a stipulated contract.

Smart contracts can have multiple applications, one of those is linked to property, and the possibility of creating around them, through these contracts, a digitalized security structure. The technology would be able in theory, to construct contractual terms and security obligations around property, turning them in actual smart property.

If we take for example a car, a simple contract would give to the owner permission for the usage of the vehicle, through the use of cryptographic keys, based on contractual terms. These applications can have many implications and benefits in terms of ownership, transfer of property and permissions to the use of certain assets.

This system can be applied to any asset whose property or usage can be granted to a person trough a contract; this includes property rights and copyrights.

1.5.6. Ethereum Virtual Machine (EVM)

The Ethereum Virtual Machine (EVM), is the execution environment for Ethereum (Ethereum community. The EVM, 2016); it is the computer system that allow Ethereum to run smart contracts and distinguish itself from the rest of the DLTs. All the active nodes of the system run the same items of the EVM, and whenever a new transaction is introduced and executed to the virtual machine, the system changes and makes everyone in the network update to the latest version of the state of the system, where the new transaction is included. Throughout this process, trust is ensured, even if a large number of calculations are required.

External actors generate inputs, or transactions, through the use of EOAs[18] at the edge of the system, and Contract Accounts can be tackled trough transactions that can communicate to one another through messages. EVM stays above them, being the system that allows for the creation of these accounts and consequently, the fulfilment of transactions and interaction among users.

EVM is a global machine in the sense that it is run by all the nodes in the system; the virtual machine is in fact spread out to all the nodes in a peer-to-peer fashion working with common account objects (Rudlang M. 2017). Interactions between objects is allowed and permitted through messages and transactions, and accounts are monitored and governed

[18] **EOAs:** Externally Owned Accounts.

by the key used by the nodes.

1.5.7. Ether

Like many other blockchain-based environments, Ethereum requires the use of an internal cryptocurrency in order to run most of its operations. “Ether” is Ethereum’s cryptocurrency, and in the Ethereum system is in fact used mostly as fuel to run operations on the platform. It is mostly used to pay fees to specific nodes of the network for the effort of participating in the consensus mechanism. Ether can be obtained in different ways; by mining, or by purchasing it from another user or third party.

1.5.8. Gas

Alan Turing in 1936, proved that it is not possible to determine before it is executed, if a computer program will run forever or it will finish running, given the description of such a program and an input.

As we know, each transaction that is executed inside the blockchain, has to be ran by every node in the system but, if the program code invoked by the transaction creates an infinite loop, this will create serious problems to the platform, immobilizing and shutting down the whole network. The possibility in fact exists that a node will generate a code that will run forever, either by a voluntary destructive act, or by an involuntary human mistake in the writing of the code. In order to avoid such an eventuality, Ethereum developed a security system for smart contracts, that makes them consume “gas”, having though a limited amount of energy for the execution of the operations.

Gas is described ironically as “cryptofuel”, and the idea behind it is to associate - to every computational step required by the miner - a cost of transaction called “gasPrice”, payed to the miner by the user that originates the transaction.

A “gasLimit” is also set before the transaction takes place. The gasLimit sets the limit for the total amount of gas that the operations involving that transaction will be able to consume. Every operation that needs to be executed will consume some of the gas at the disposal of the transaction. If some of the gas is not consumed by the miner through the computations, the remaining fuel will be sent back to the originator of the transaction. If during the computation, the gasLimit is reached; the transaction is cancelled but the gas used, goes to the miner anyway.

This system allows for the interruption of any computation that might result in a loop and might immobilize the system; since eventually, every computation will run out of fuel.

These precautions will discourage some hackers from attaching the platform. This system makes it impossible to create infinite loops, but it still allows for very big ones that will slow down the system and give time to malicious users to take advantage of the temporary stall of the network. In the section about the Security of Ethereum[19] we will go further into details on this topic.

With the introduction of this fee for mining, miners are not de-incentivised to undertake harder and longer calculations, since the effort for such mathematical calculations will be fairly rewarded.

Gas price is dependent on the amount of computation required, and by the agreement between the miner and the user of the transaction. It cannot be defined as a standardized Ether amount, also because of the heavy volatility of cryptocurrencies in the free market. Miners are also entitled to avoid computations that offer a to low gasPrice; this creates a market for computation and gas.

1.5.9. Consensus Protocol in Ethereum

As we seen in the consensus section[20]; consensus consists in the mechanism that is created between nodes, in order to determine which blocks are to be considered authentic and true, and which are not. In the Bitcoin system we know that the consensus mechanism is called Nakamoto consensus and it follows the rule of:" The longest chain wins". This system though, may delay the broadcasting of the authentic blocks to the rest of the system, affecting the security of the whole network. According to Yonatan Sompolinsky and Aviv Zohar (Sompolinky Y., Zohar A., 2013) in the time between the completion of a block and the broadcasting to the rest of the network, the system is vulnerable to possible attacks, and delays in the propagation of the bocks may have serious security issues. We can identify two major factors that influence the possible creation of this state and they are "Block creation rate" and "Block size".

Block creation rate refers to the time interposing between the creation of two blocks.

Let's assume that the time to broadcast a new block to every node is always the same ad fixed; if we reduce the time that exists between the creation of one block and the other, we will put the system in a not secure situation more often, increasing the time in which the system is vulnerable to possible attacks. In Figure (2) below, we can see the black arrow as the time necessary to reach all nodes and in which the system is in a vulnerable

[19] Section: 1.5.10 Security
[20] Section: 1.4 Consensus and Mining

state.

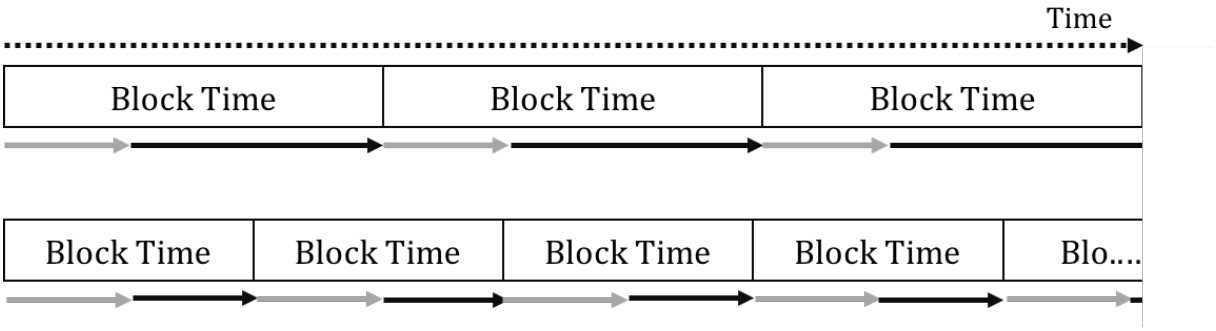


Figure (2): Shorter block time

Block size on the other hand refers to the volume of information embodied in each block. Whenever a new block contains a lot of information, it will take more time to broadcast all that information to all the nodes in the system, this will increase the delta of time in which the systems is vulnerable. The black arrow in Figure (3) shows the difference that Block size makes in making the system more vulnerable.

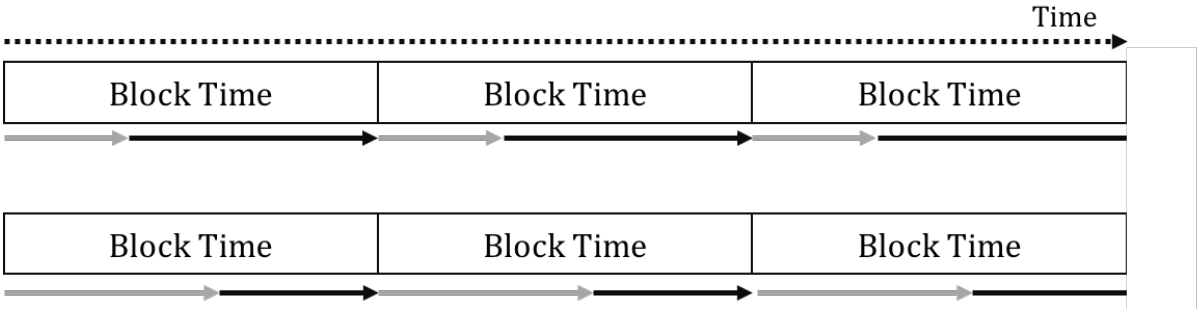


Figure (3): Bigger block size.

These assumptions make sense in a system where all nodes have the same computational power and are able to transfer equally well the information between other peers. Vitalik Buterin (Buterin V., 2014) point out though, that there is a substantial difference between different nodes, in terms of both computational power and centralization with respect to other nodes; this means that some nodes are more likely to produce new blocks and be able to receive them faster as well as broadcast them faster inside the network. For these reasons, Ethereum uses a different system to achieve consensus without impacting the security of the system. This system is called: “The Greedy Heaviest Observed Sub-Tree” commonly referred to as GHOST. First introduced by Sompolinky and Zohar, GHOST differs from the Bitcoin consensus system in the sense that: “the heaviest sub-tree wins”,

rather that, “the longest chain wins” (Sompolinky Y., Zohar A., 2013). With “the heaviest sub-tree wins” we refer to the tree with the most computations work related to it. So, whenever a fork, or a split from a block occurs, the sub-chain that should be selected as true according to Ethereum is the one that is not necessarily the longest, but the one with the highest number of blocks generated below it and related to it. Figure (4) shows the differences in the selection of the sub-tree for the two different networks.

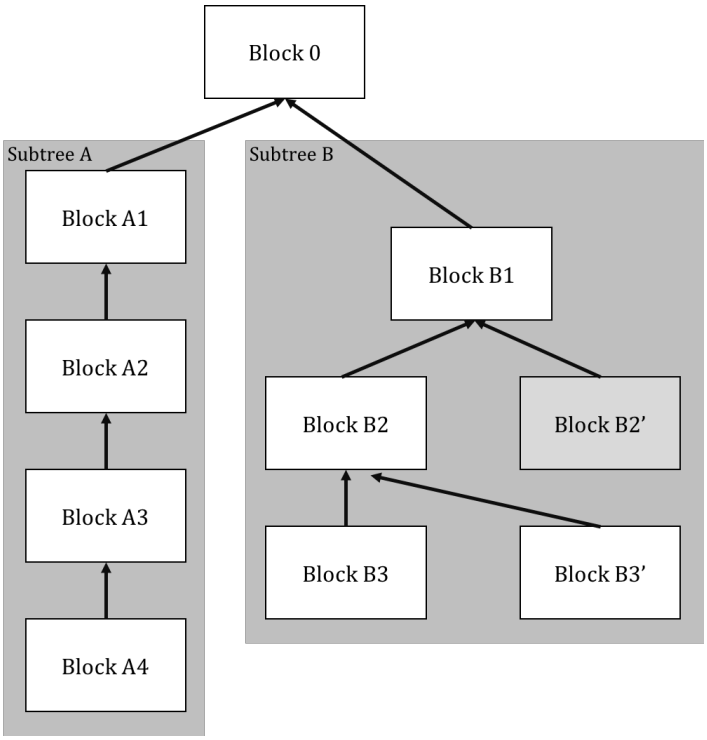


Figure (4): Subtree selection differences.

As we can see, a fork has been created starting from “Block-0”, creating two sub-tree called “Subtree-A” and “Subtree-B” with different depth, respectively 4 and 3. According to the Bitcoin or Nakamoto consensus, Subtree-A should be selected because of the higher depth. In the case of the Ethereum consensus mechanism on the other hand, Subtree-B will be selected because of the higher number of blocks associated with it; it is in fact the heaviest subtree between the two. Block B2’ is called a Ommer Block, and it is created by smaller miners that would continue to mine on a block even if another valid block has been created; since these new valid blocks may take more time to reach them. In order to avoid wasting the mining effort given by these smaller miners, the work created, is added up to the system to increase the tree size. The miners that create the Ommers are reworded for their computational effort, even if it is a fraction of what the miner of the

globally recognize block is been given. The maximum level of depth of a subtree allowed is six, and the maximum number of Ommers allowed inside a tree is two (Rudlang M. 2017).

1.5.10. Security

The dependency on global consensus inside the blockchain system, creates some security flaw in the network. One of the most known type of attack is the "51%" attack considered to be the most dangerous treat to the security of the system.

As we have seen before, in order for a transaction to be recorded on the blockchain, consensus by all miners has to be provided. This means that the introduction of a malicious block or transaction would be spotted by the network and rejected; unless a group of mines together would be able to control 51% of the total computing power of the network. This would mean that those holding the 51% of the mining power, would be able to create a fake malicious block that could not be rejected by the rest of the miners being them in numerical disadvantage. The attack could change the rules of the blockchain, creating programs that benefit that 51% majority.
The creation of such a situation would require an immense computational power, that not even pool of miners[21] could gather. It is interesting to notice though, that the free and open nature of the network could theoretically allow for such a scheme, since no authority exists that would prevent such an attack. It is important also to notice that if, such a circumstance would come to happen, the system would recognize the treat and abandon the platform, that would be permanently compromised, leaving the attacker with a useless network.

The "Long Range Attack" (Buterin V., 2017) is an adaptation of the 51% attack, that allows for the slowing down of the authentication process by miners, allowing a hacker to have the time to develop its own block and attach it to the chain. In order to do so, an hacker would have to slow down the rest of the validating nodes, creating a very complicated transaction, to which only he or she has the possibility to activate specially designed trap doors[22] and get ahead of other miners. This would allow him or her to attach to the chain

[21] **Pool of miners**: A large group of miners that put together their computing power to win mining races.
[22] **Trapdoor:** consists in an unknown entry point inside a computer program that allows only the creator of the program to have access to specific sections without the conventional process of identification.

a block inside of which there are contracts or transactions that would vote in his or her favour. The attacker can in fact re-write the blockchain, while the rest of the miners are occupied executing the long loop transaction.

As we know the Ethereum system allows user to write their own contracts, programs, and applications that are put on the blockchain; these programs may or may not have security flaws depending on how well they are programmed and written. The possible presence of bugs could be exploited by malicious users and undermine the stability of the contracts.

There has been a case in which an unintentional loop hole in a smart contract in an Ethereum instance was exploited by a hacker. The hacker was able to withdraw from this company called "The DAO", a significant amount of money (Buterin V., 2017). The contract of the "The DAO" worked as it was programmed to do, but unfortunately who programmed it did not realize that it could have been used against them. Users in the system realized that the The DAO had been hacked and most of them agreed to make a so called "Hard Fork", that created a new block in contrast with the malicious block created by the hacker. This new block was recognized by almost the majority of the network and the money stole went back to the original owners. This hard fork, created a split in the blockchain, creating two different network, "Ethereum" and "Ethereum Classic", that contain the same information until the moment of the attack. Both chains now work and have their own users, but work in parallel, without any interactions.

The hack of the The DAO was a warning sign for those that want to construct smart contract. Buterin (Buterin V., 2016) in the Ethereum blog reassures users that even if the platform is perfectly safe and allows for the creation of perfectly functioning smart contracts, it is still necessary to pay particular attention to the presence of possible bugs inside contracts. There are on-line companies right now that can help users create safe and sound smart contracts and prevent these hacks form happening in the future.

1.5.11. Scaling on Ethereum

Unlike the Bitcoin network, Ethereum contains not only transactions, but also the information on the latest state of the contracts written on the Ethereum platform. This will create a serious issue for scalability of the platform. One of the solutions to this problem is the fact that Ethereum nodes, can have different roles and store just some sections of the state, and not the full blockchain history (Buterin V., 2014); only active

nodes in fact must store the complete blockchain, like in the Bitcoin network. The original Ethereum protocol does not force all nodes to store the whole blockchain in order to validate transactions.

With this arrangement, there is though still the problem of the centralization of information. Full nodes, as the size of the blockchain increase, may become fewer and fewer, creating the opportunity of working together to use the platform at their interests. In order to cope with this problem, Ethereum uses a verification protocol, creating a "proof of invalidity" that will avoid verification of invalid blocks.

1.6. The potential of Ethereum

Now that we have some knowledge of what a blockchain is and what are the functionalities of this new technology, we can try to define what might be its possible applications. The potential of the technology in fact, goes beyond the mere creation of cryptocurrency. Application of the technology can space across finance obviously, public records, private records, physical assets keys, business, government, and many other industries.

The Legal Profession:

The legal industry is facing a transformation leaded by the use of blockchain technology, and more specifically, by the introduction of the concept of smart contracts. Through this technology, some aspects of the law can be digitized and converted from legal prose to flawless code.

Currently, the legal system and its bureaucracy creates tons of paperwork which is hard to keep track of. Each action, transaction or legal act has to be recorded and stored in order to have an actual proof of what happened and who were the actors involved. The blockchain technology offers a system in which any interaction or change of state in an asset can be recorded and remain in the ledger for ever. This will reduce drastically administration costs and reduce time needed to gather necessary information about single cases. The introduction of the technology in this environment could be a game changer that would help the creation of a better, more transparent and consequently fair system.

We need to keep in mind that blockchain technology and functionalities, cannot be applicable to every aspect of this environment. The technology can, and probably will be applied to those tasks that can benefit from being automatized.

When it comes to smart contracts, what they can do is not substitute the already existing structure of laws, but they can help in the creation of trust between the parties involved. With the creation of new markets, will come the creation of new needs, in which smart contracts will certainly play a central role in the definition of relationships and trust.

Clearing & Settlement:

The use of the blockchain the Clearing & Settlement services - usually offered by financial institutions and third parties - is probably the most interesting and useful application of the blockchain in the financial sector. The "Fintech" industry is in fact the world in which the DLT technology has been applied and studied the most. These activities usually cost billions to financial institutions every year, and financial giants like Santander[23] believe that this technology will save the industry billions in the next few years.

Some of the major benefits of the application of DLT technology in the field of payments. Clearing and settlement, could tackle the issues that have been part of the industry for quite some time; these include: end-to-end settlement speed, data auditability, resilience, and cost efficiency. The promise of the resolution of these problems led the industry and its actors to investigate on the potential of the technology and its possible benefits. The technology could change drastically the industry and the way in which payments and other financial services are provided.

The technology is not fully developed yet at this point in time, transactions in fact could be faster, and scalability is still an issue; but many financial companies are investing in it and will soon make their developed solutions public (Mills, David, Wang K. , Malone B., Ravi A., Marquardt J., Chen C., Badev A., Brezinski T., Fahy L., Liao K., Kargenian V., Ellithorpe M., Ng W., Baird M., 2016).

Smart/Digital Assets:

The technology around blockchain, allows for the creation of the so called Smart/Digital Assets. A smart asset can be defined as a property, whose ownership is controlled through a blockchain and they can be transferred using contracts; this allows for a rather costless and trust-less transfer of the ownership of assets. Transactions and transfer of property, through the use of smart assets, will reduce substantially transaction fees and would allow trades that would have never been possible without the technology behind it.

[23]http://www.santanderconsumer.it/prestiti?gclid=Cj0KCQiAyZLSBRDpARIsAH66VQKkUEcGphSjM6aALj6DlbiB5iJY6jEsTjA-uV5h55uyy5vAKoNpmQUaAvtzEALw_wcB

The technology allows only those in possession of the key to be entitled to the ownership of the asset. This application will also change the way in which loans and collaterals are distributed and collected, since the ownership of anything can be traced easily in the public blockchain.
Those that will invest in this sort of system now, are believed to have an advantage in the future for what concerns property rights, traceability of assets, and proof of ownership of those assets.

Digital Identity:
Every individual in order to interact digitally with the rest of the world, must rely on digital identity in order to be recognized and in order to recognize the ones he or she is interacting with. However, the state of the art in security for digital identity, makes it hard to trust the person we are interacting with thought the internet, since it is fallible and disjoint; and furthermore centralized and costly. The introduction of the blockchain technology will allow for the creation of a digital identity that is unique, trustworthy, not managed by few individuals that hold our private information, and secure. This will empower people to be entitled of their own identity and share it between other trusted individuals in a trusted network.
This will improve customer protection, and security, while having control over personal data to be disclosed to the public; while on the other hand will allow businesses to reduce the risk and the cost of storing sensible information on their servers. On the regulator side although, it will help them to standardize processes, while increasing efficiency and quality of their work (IBM, 2017)[24].

Voting:
Traditional voting systems can be considered risky in the sense that a paper-based system can be modified by malicious auditors, and it is costly to manage and keep track of all the information associated with it. It currently exists a type of digital voting, that still is centralized and managed by a single entity and a single server. This allows for the creation of a single point of failure; a single storage of information that can be hacked and modified by malicious users or by the trusted third party itself.
It is necessary to create a system that would be digitalized, secure, transparent and

[24] https://www.ibm.com/blockchain/identity/

flawless, in which information about votes can be stored and impossible to be modified. With the introduction of the blockchain technology in the voting system, these characteristics are met and can create a secure system in which voters can be sure their information and their will is being pursued.
The system would allow for a clear and precise representation of the will of the voters. This system can be applied in any situation in which the voting rights can or has to be implemented, meaning that it can be implemented in the government system as well as inside a corporation where the will of the shareholders should be pursued.

Healthcare:
One of the major problems in the healthcare system is the inability or the difficulties for different hospitals or platform to share information about patients (Collen M.F., 2011). this limits the knowledge for medical institutions and doctors of the conditions of a patient that has been treated in their institution for the first time. The introduction of the blockchain technology could change this trend, by allowing not just for a clear definition of the patient's medical history, but will also allow for the creation of a database where all the information about different cases would be stored, creating a learning platform for doctors, and possibly a learning artificial intelligence.
Obviously, the information related to each patient would be protected and through the use of digital identity, is the patient that will decide who will be able to see his or her medical records and especially what they will be able to see.

These are only some of the possible applications and the improvements that this technology is bringing to the table. But as we can see, concepts and the structure behind it, are able to change positively and substantially many of the aspects of our lives.

In the next chapters, we will take a closer look of one of the possible application of this technology and we will see how the implementation of the blockchain will improve that industry and even be able to create many new side industries that will compensate some of the current issues we have with the traditional methodologies.

CHAPTER II

Traditional & Equity Crowdfunding Mechanisms, Limitations, and Potential

In the creation of a new venture, raising capital for an entrepreneur may be hard with traditional methods of funding. Credit can be uncomfortable to carry especially for a new venture. Crowdfunding tried to solve this problem by creating specific internet platforms, on which a person or an organization could raise capital from the crowd for a particular venture. The objective is to be able to raise small amounts of capital from many members of the network forming the crowd.
The reward for contributing to the capital raising can be different depending on the typology of crowdfunding used.
A possible definition of crowdfunding can be the following by Belleflamme (Belleflamme P., 2013):

"Crowdfunding involves an open call, mostly through the Internet, for the provision of financial resources either in the form of donation or in exchange for the future product or some form of reward to support initiatives for specific purposes."

Belleflamme, 2013

This definition may be criticized since it does not take into consideration the goal of the investors and the creator of the venture.
Those who seek to collect the money, may be doing it to collect small capitals for a single activity or in order to create a new venture. The use of crowdfunding can also prove the validity of an Idea, that would allow for the raising of external capital by someone outside the network. These platforms and structures can also be used in order to promote business activities and raise interest for organizations in the development stage or creation.
Collectors might be seeking to raise a small amount of money for a one-time project or to find seed capital for a start-up business. Furthermore, crowdfunding has been used by collectors to show a potential demand for their idea which can lead to increased funding

from other traditional sources. Crowdfunding has also been used for marketing, to create interest for the project at an early stage.

In this chapter we will focus not so much on the different typology of crowdfunding, but on the specific Equity-Based platforms that allow for such an innovative way to raise capital. This new method is contraposed to the traditional one of Venture Capital and presents a series of advantages and characteristics, that are changing the way funds are raised by small and independent ventures. In this chapter we will analyse the different advantages and disadvantages of the system and especially how important trust is for both parties involved in these transactions that investors and the entrepreneur face.

2.1. Crowdfunding Platforms and Intermediaries

Crowdfunding platforms cover the third party role, staying between the two side of the transactions during the process of raising capital. The platform's role can be considered as the one of the middleman, even though, it does not participate directly in any capital raising campaign.

Platforms of such sort, participate indirectly in the campaigns, offering a list of services to both the collectors of the funds and the contributors, in order to make the relationship as easy as possible, as cheap as possible and as secure and riskless as possible.

They offer a platform of communication between investors and entrepreneurs, where communication between the two parties is allowed directly; secondly, they allow for the creation of a pool of possible investors from which entrepreneurs can have access to. It is a group of people that declare to the platform their willingness to participate in interesting and profitable opportunities. Furthermore, these platforms allow transactions to occur between investors and new ventures in order to raise capital; and finally, they are able to close down possibly dishonest projects, but at the same time, can decide to sponsor other ones that particularly interest them. These platforms are in fact able to create good conditions for entrepreneurs to raise capital and be able to create new ventures (Agrawal A. K., Catalini C., Goldfarb A., 2011).

They also provide the investor with a list of possible campaigns from which to choose from, and most importantly, they are entitled of legitimizing the crowdfunding market; meaning that they play the role of the trusted third party, necessary to allow the flow of transactions between the two parties involved. One of the most important roles in fact, is the service of due diligence they perform on the proposals of fundraisers. This is the most interesting characteristic, that distinguishes them from the traditional form of

crowdfunding, in which any idea can be presented to the investing public, regardless of its validity.

2.2. Equity based Platforms and Different Business Models

The presence of more than one agent that interacts through an intermediary, characterize the creation of what can be defined as a multi-sided market (Rysman M., 2009). In the case of the crowdfunding market, these agents can be called capital-seeking and capital-giving. In this environment, the role of the intermediary that allow for the interaction between these two agents is played by the crowdfunding platform. Through a crowdfunding platform, the two agents are able to connect and avoid possible asymmetries in information and reduce largely costs of transaction (Mahadevan B., 2000). Platforms are financial intermediaries, that play the role of two-sided financial allocators in a market composed by capital-giving and capital-seeking actors.

Financial intermediaries are able to offer financial services that can be described from a functional perspective, and divided in three sub categories of services, that are: Lot Size Transformation, Risk Transformation and Information Transformation (Hass P., Blohm I., 2014).

Lot Size Transformation:

These intermediaries provide services in order to accumulate capital and they make it easier for the actors involved to have access to it. They allow the exchange of goods by creating ad hock payment systems and mechanisms for the accumulation of resources between businesses; regardless of the geographic locations, and time (Merton R. C., 1995).

Risk Transformation:

Financial transactions are associated with risk, created also by the possibility of free riding by capita-giving agents. Financial intermediaries are able to manage and reduce significantly costs of monitoring, through diversification and increasing of such activities. This means that in the field of financial transactions, they perform and act in such a way that reduce the risks associated with financial intermediation (Gorton G., Winton A., 2003).

Information Transformation:

Intermediaries can reduce information asymmetries in the sense that they create a bridge between the one that hold the information about the projects, meaning capital-seeking agents; and their counterpart, meaning capital-giving agents. Intermediaries hold the trust with the former and are, by doing so, creating information (Gorton G., Winton A., 2003).

On a Crowdfunding website, the two agents interact on an internet based platform that is able to reduce transaction costs, monitoring costs, and enhance the interaction and pairing of agents. Intermediaries though, through these platforms face different challenges with respect to the ones faced by traditional financial intermediaries. In fact, internet platform does not perform the act of borrowing and lending capital per se; in fact, their core activity is to reduce information asymmetry and reducing transaction cost between the two parties (Mahadevan B., 2000). Crowdfunding platforms are able to take advantage of the dissimilarities in information bulks, and the global distribution of the agents composing the market. What platforms are also capable of doing, is giving both sides some degree of guarantee and trust in the platform, which helps reducing the risk associated with money transfers and capital accumulation (Mahadevan B., 2000).

We can also say that crowdfunding platforms have changed the role of the traditional financial intermediator in what we defined earlier as a two-sided market.

Table (1) (Hass P., Blohm I., 2014) shows precisely and in a graphical way the differences between the two models of financial intermediation.

Functional Characteristics of Equity Crowdfunding as a Financial Intermediary		
Function	**Financial Intermediaries Implementation**	**Equity Crowdfunding as Financial Intermediaries Implementation**
Lot size transformation	Payment systems for exchange of goods and services (Merton R. C., 1995). Mechanisms for pooling funds (Merton R. C., 1995). Transfer economic resources through locations time and businesses (Merton R. C., 1995). Provide liquidity (Gorton G., Winton A., 2003).	Allowing for the interaction and matching between agents and enable funding (Belleflamme P., 2013). Provide the service of an economic market for the exchange and return of capital (Bakos Y., 2000). Allowing for capital-giving and –seeking agents to overcome time, space, communication, and business limitations (Bakos Y., 2000). Demand and funding mechanism regulation (Bakos Y., 2000).
Risk transformation	Managing risk and uncertainty (Gorton G., Winton A., 2003).	Assessing credit of the capital-seeking agents. Pre-selection of projects. Acting as a trusted and incorruptible third party, objectively disassociated (Bakos Y., 2000).
Information transformation	Handling asymmetry in information (Merton R. C., 1995). Provide price information and information production (Merton R. C., 1995).	Accumulating information. Providing information about projects for capital-giving agents (Mitra T., Gilbert E., 2014). Functioning as an electronic market place creating a relationship between the two parties involved and allow for the exchange of information (Mahadevan B., 2000).

Table (1): Differences in terms of functions between Traditional Financial Intermediaries and Crowdfunding as Financial Intermediaries.

Different crowdfunding platforms can have distinctive business models depending on how they want to tackle the market and create revenues; and on what type of regulation they need to apply to. What all platforms have in common on the other hand, is the fact that they want to manage relationships between the actors in the two-sided market; meaning that they want to offer "project-regulation" and "fundraisers-screening" services.

The typology of fundraisers and funders may determine the approach and the pricing policy of the service provider. Each platform needs in fact to attract possible customers to

enlarge its customer base and the scope of the platform, and not just being more competitive, but also offer different useful services to final users. The perception of the validity of the platform in fact, is related also to the within-type and across-type external effects; this is why most intermediaries use the following revenue stream (Bellaflamme P., Omrani N., Peitz M., 2015), (Bellaflamme P., Omrani N., Peitz M., 2016):

1. The platform can hold interests on the funds raised while the campaign is being processed. In fact, the funds raised are not delivered to the fundraisers, until the completion of the campaign.
2. Fundraisers may be required to pay transaction fees to the platform; in most cases the payment of this fee is required only if the designated amount is reached.
3. Charges can be made on support services offered by the platform.

In the case of crowdfunding platforms, this system is what most platforms use; they will hold a percentage on the raised capital by new ventures as fees for the services provided. In the figure below (Figure (5)) we illustrate the general model used by these platforms (Bellaflamme P., Omrani N., Peitz M., 2016).

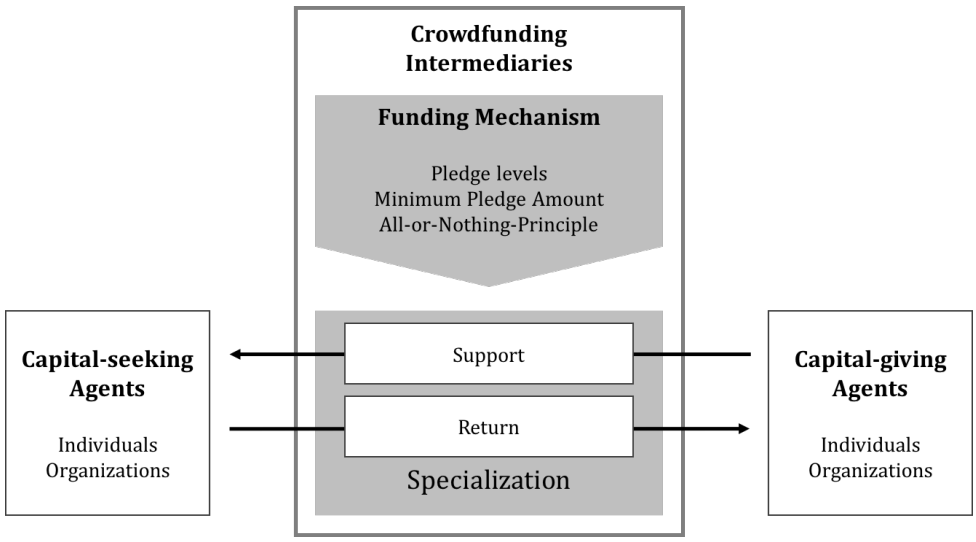


Figure (5): Crowdfunding platform business model illustration.

The next subsection is dedicated to the presentation of three different peer-to-peer contribution mechanisms that are used to create crowdfunding models. The three represent the most diffused models in the market. The IOSCO Research[25] gives a

[25] https://www.iosco.org/

description of the models that led to the creation of these synergy models (Kirby E., Worner S., 2014).

The interaction between the two parties and the degree of involvement of the intermediary as a trusted external partner are the two variables that define the differences between the three structures that will be described. The level of involvement of the platform is extremely important in differentiating crowdfunding websites from one another. The differences in the interaction models, movement of money, and the different interactions between parties involved will be explained through this section also with the use of graphs for a better understanding.

2.2.1. Peer-to-Peer Contribution Mechanism

Peer-to-peer lending procedures come into play when a bank or another financial institution denies credit to a possible entrepreneur.

The case might occur when instead of a central and singular institution willing to absorb the risk of the creation of a new venture, a group of people is willing to share the liability forming what is commonly referred to in the milieu as the "crowd". We should also keep in mind that every loan is associated with a level of interest rates or payments at maturity, which is tackled differently by crowdfunding platforms and by banks.

Separate Account Model:

The first peer-to-pee model we analyse is called the "Separate Account Model".

The two actors in the market have distinct accounts on which they manage respective funds. What the platform does is to connect them through the creation of a contracts that hold a third legally separated and protected account, storing the amount raised by the campaign. In this case the platform constitutes a trustee of the account and we can see from the Figure (6) (Kirby E., Worner S., 2014) the graphical description of such a model:

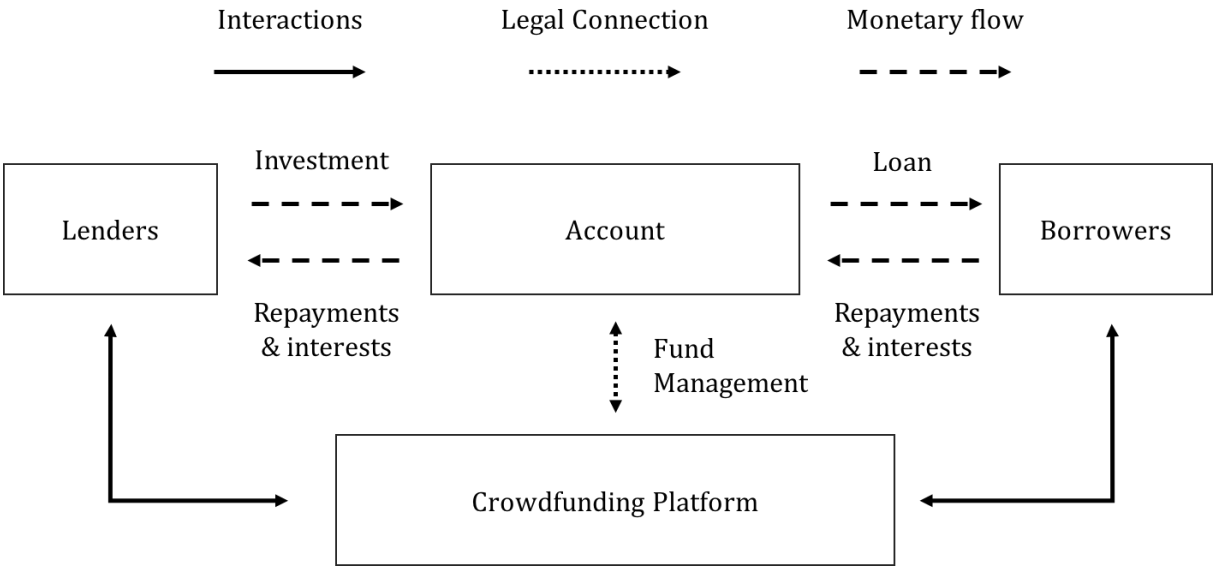


Figure (6): Peer-to-peer "Separate Account Model" interaction illustration.

Notary Model:

The second peer-to-peer model we analyse is called the "Notary Model". This system leverages on the use of what are commonly known as public bonds. Whenever the lender is put in contact with the borrower through the platform, he or she is able to invest in the new venture and is accredited with the right to the repayment of the loaned amount; this concept is similar to the concept of the investment security. A bank may be authorized to manage the credit, while the funder still holds the risk of the investment. The figure below (Kirby E., Worner S., 2014) (Figure (7)) represents the notary model just explained.

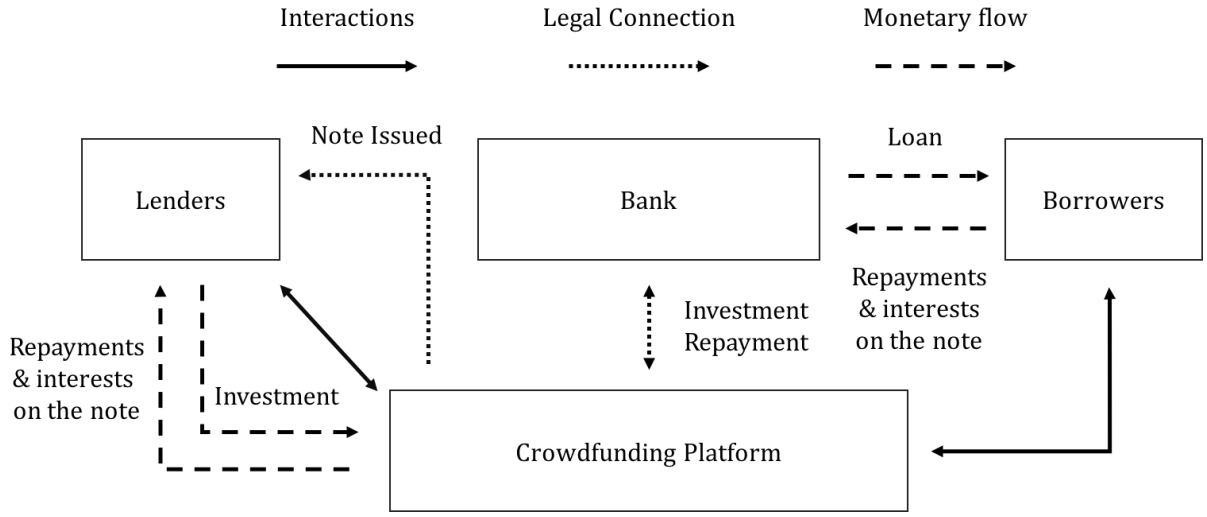


Figure (7): Peer-to-peer "Notary Model" interaction illustration.

Guarantee Model:

The third peer-to-peer model we analyse is called the "Guarantee Model". What characterizes this lending model is the fact that the investments are not made directly by the funder, but by the platform itself. The intermediary in fact, can guarantee a previously determined rate of return on a previously set amount, that the lender can decide to put at risk. The money used to finance new ventures is extracted from a fund, in which a group of investors accumulated a certain amount. By putting money in that account, funders agree for that amount to be invested in different ventures, regardless of the venture in which those funds will be put into. The decision on which ventures to fund, is in the hands of the platform trusted by the funders. The figure below (Kirby E., Worner S., 2014) (Figure (8)) represents such a model.

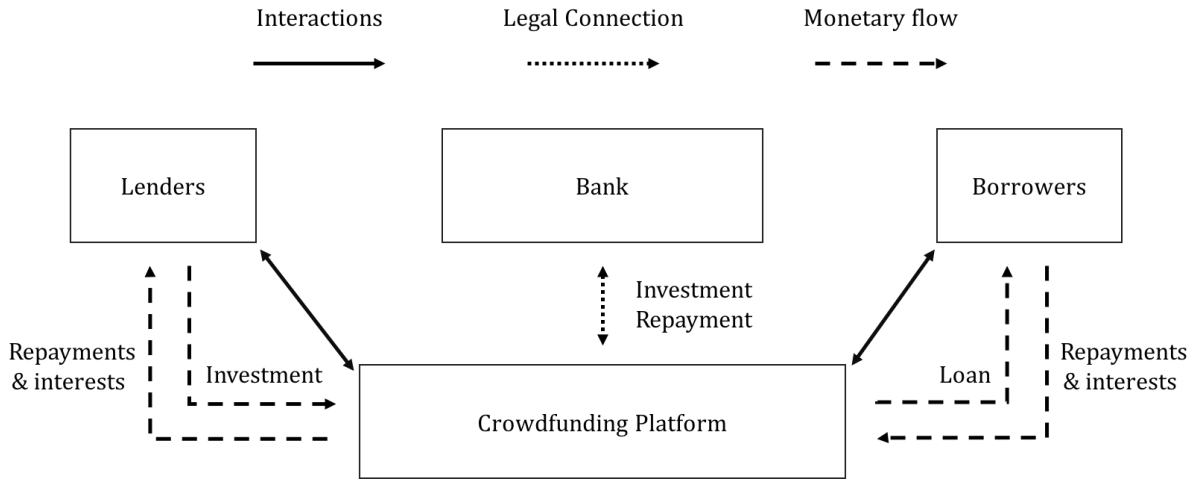


Figure (8): Peer-to-peer "Guarantee Model" interaction illustration.

As we can see, these peer-to-peer models are the first step into the interaction between equals; in a system in which people that need to interact, do not trust each other. There is willingness to interact with one another, but the level of trust is too low for this interaction to happen especially on an internet platform. This is one of the reasons why the equity crowdfunding platform is utilized, in order to guarantee a certain level of eligibility of the market and helps reduce the level of risk associated with the low trust.

2.2.2. Equity-Based and Royalty-Based Models

One of the most interesting forms of crowdfunding, is also the less utilized. Equity or Royalty based crowdfunding models in fact are mostly theoretical, since very few actors have decided to use their platform in such a way. This method allows for investors in

crowdfunding campaigns to receive not just a reword, like in the most common crowdfunding platforms, but actual shares of the company they decide to fund. Different models are characterized by dissimilar regulations on equity right for funders, depending on the typology of the system implemented.

Revenue and profit sharing, direct equity and convertible bonds are common mechanisms used by these platforms, and the utilization of these tools vary depending on the approach each platform decides to undertake. The next few paragraphs will describe a few interaction models to choose from when creating an equity based platform, depending on the level of involvement as a third party that the platform decides to undertake.

Low Responsibility Model:

The model we present first, is characterize by "low responsibility" undertaken by the equity crowdfunding platform, in the role of the third trusted party. The intermediary's role is to create a relationship between the parties involved, granting the investor legal claims on a percentage of future profits, revenues, as well as royalties depending on the terms of the contract. The platform can also administer equity, making investors eligible for voting rights, or ownership of shares (Kirby E., Worner S., 2014). The figure below (Figure (9)) shows graphically such a model.

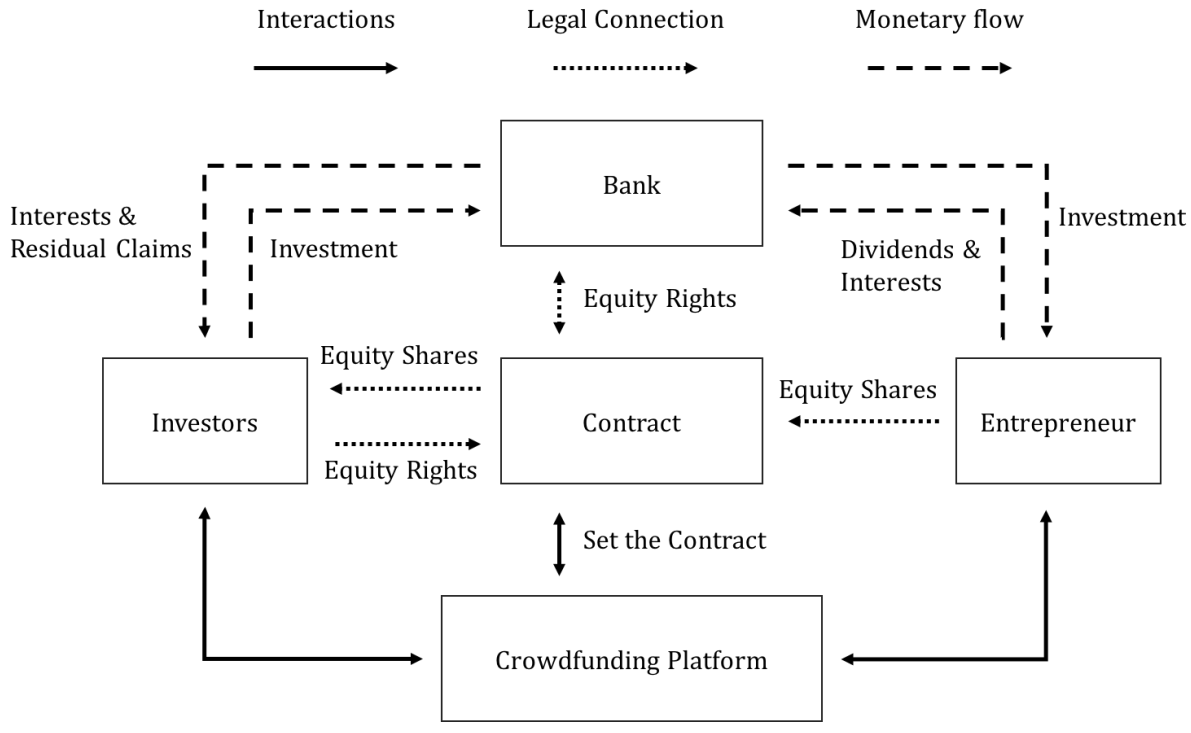


Figure (9): "Low Responsibility" model for an equity-based crowdfunding platform.

Medium Responsibility Model:

In the second model, the intermediary is able to offer the service of detention of the investment legal title in favour of the investor, that continues to be the rightful possessor of the shares. This model is characterized, for these reasons, by a higher degree of responsibilities to be undertaken by the platform. The figure below (Figure (10)) gives a graphical representation of such a model.

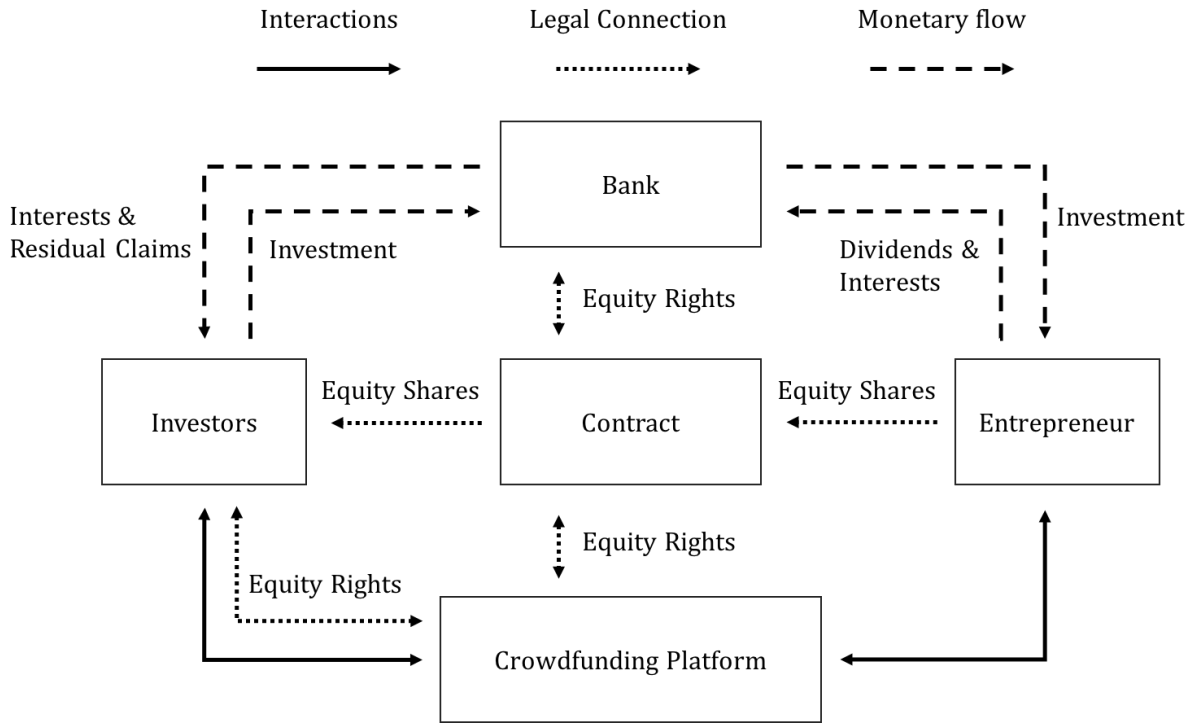


Figure (10): "Medium Responsibility" model for an equity-based crowdfunding platform.

High Responsibility Model:

The model that features the highest level on interaction by the third party platform is the following; in which the platform, based on contractual agreements with investors, is entitled to make investment decisions and hold shares. The figure below (Figure (11)) shows the graphical representation of the model.

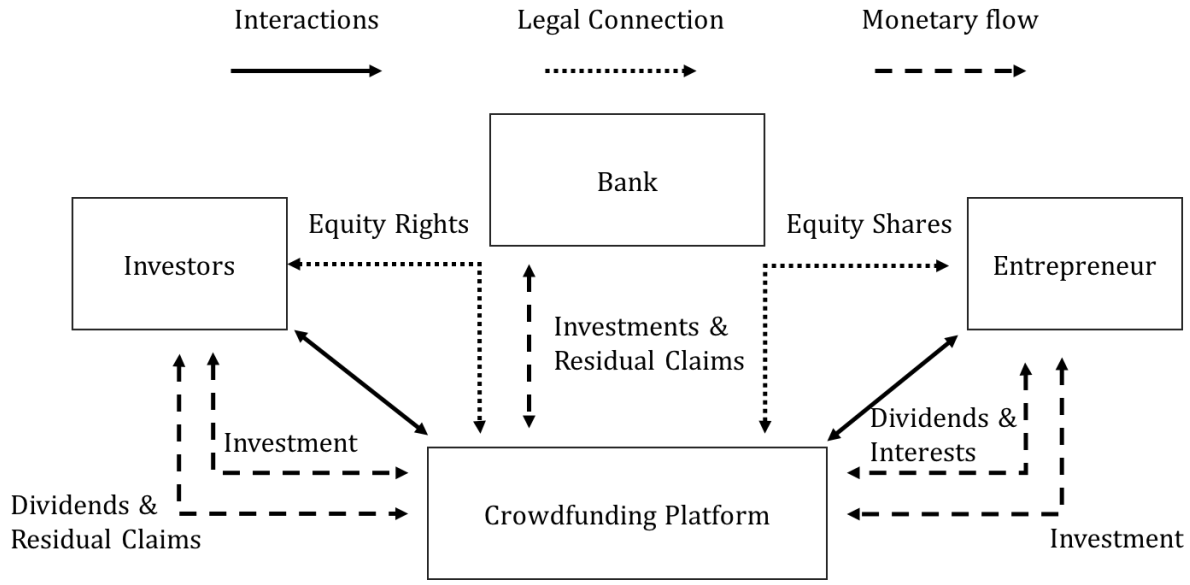


Figure (11): "High Responsibility" model for a, equity-based crowdfunding platform.

This was a general description of the different models associated with the different levels of involvement of the equity crowdfunding platform in the financing industry in which it operates.

We would like to note the level of involvement of the bank in such a system. A financial intermediary such as the bank, is always present and has a central role in the interaction between the parties involved. The financial intermediary is one of the holders of trust, and the reference for issues that regard the borrowing and lending of value. It is important to remember the role of banks in the network, especially when we will talk about the differences with the system that the introduction of the blockchain technology will introduce[26].

2.3. Different Service Models

Crowdfunding platforms have developed through the years, differentiating from one another especially in the type of services they offer to both investors and developers. What needs to be taken into consideration when designing a new platform in fact, is the type of services it wants to provide. In order to understand better the economy behind crowdfunding than, in this section we analyse the decomposition of the services offered by crowdfunding ecosystem, into single components (Haas P., Blohm I., Peters C., Leimeister J. M., 2017).

[26] CH III

2.3.1. Service Modularization

"Modularization is the decomposition of one object into decoupled single components with specified interfaces that can be combined to create new single object configurations"
(Haas P., Blohm I., Peters C., Leimeister J. M., 2017).

By decomposing services provided by crowdfunding institutions, we can create single modules that can be studied. These services can be separated, recombined, and hence form new and different services. Modularization has two major principles to keep in consideration in the definition of the single services; these principles are "Cohesion" and "Loose Coupling" (Haas P., Blohm I., Peters C., Leimeister J. M., 2017). Cohesion refers to the necessity of the modules to have defined levels of complementarity between one another; Loose Coupling on the other hand refers to the fact that single services must not depend on each other.

2.3.2. Service Modules for Crowdfunding

Through the study on the modularization of services provided by crowdfunding platforms and ecosystems around the web, we are able to identify a list of modular services (Haas P., Blohm I., Peters C., Leimeister J. M., 2017) that, in the next chapters, will help us support a comparison between web-based crowdfunding platforms, and blockchain-based platforms.
Here below we present a brief explanation of the major services that a crowdfunding ecosystem can offer to users, useful for both sides of the market.

Matchmaking:
The main obvious role of a web platform is to be able to connect the two sides of the market, meaning capital-seekers and capital-givers. This is done in order to spread information, and register capital transfers and funding activities.
The platform is able to create a bridge and a link between those that are willing to invest in new, even if risky new ventures, and those that are in need to accumulate capital for to start a new business.

Contracting & Compliance:

Once the target funds are reached, the platform can legally validate obligations and conformity through the issuing of a standardized digital legal contract. Each platform can have their own standardized type of contract to be presented to the company or the investors. The conditions stipulated in the contract between the three party may depend on many factors including the type of industry in which the company is or will be operating, and the amount of capital to be raised.

Customer Support:

Through the platform, the two actors in the market can interact with each other more easily. Certain services are provided in fact, to improve relations between the parties by lowering or clearing up obstacles between them and resolving concerns.

When investing small or conspicuous amounts of money, investors must feel at ease in the interaction with the fundraiser and the platform. It is in the interest of the platform to make the transactions and the communications between the parties as smooth and as transparent as possible

Risk Scoring:

In an equity crowdfunding platform, risk associated to capital seekers is tracked and ranked. This information refers to the trustworthiness, project history, credit, and also project descriptions and validity associated to the capital seeker.

The attribution of a score to the capital seeker is of most importance for the funders, especially for those that are not able to do it by themselves a well-defined due diligence of the project they are being presented.

Some companies perform internal due diligence and present to the fundraisers a score for the projects based on their experience in the field. Other companies, in order to avoid conflicts of interests, prefer to let other third parties perform the due diligence for them. These impartial parties are sometimes the best choice in situations in which the expertise of the platform may not be enough to determine the feasibility of some projects.

Authentication:

Identification and authentication is necessary and thoroughly applied on these platforms. The use of authentication is useful to all users in order to comply with regulations, and

create a safer environment for clients, in which they know exactly who they are interacting with.
Information about investors and funders are analysed deeply and securely stored; this creates a more trustworthy and transparent environment.

Crowd Activation:
Propagative and educational activities are performed by these platforms in order to create on their network a valid pool of clients. A larger number of clients willing to invest in new ventures, will ensure a higher rate of success for proposed projects; with the consequence of the activation of a network effects.
The use of crowdfunding and equity crowdfunding in particular, is changing the target for the financing industry. In the past, only the ones that had access to sufficient amount of money to finance significantly new ventures, were able to participate to the market. The use of crowdfunding is moving the attention to the consumer market, where there are nonetheless individuals with lower capital availability, but still with a high willingness to undertake financial risks and invest in new ventures.

Investor Relations:
Constant interaction and communication on the performance of active projects is disposed between the parties involved. These precautions are implemented in order to maintain a transparent and democratic platform; and it is done through the use of specially designed on-line tools.
The level of communication is determined both by the platform itself and by the firm. The communication interaction can be limited to the period in which the campaign is been developed or even after the campaign is over, depending on the agreement between the parties.

IT Operations:
It is fundamental, in the case of an on-line service platform, a proper, well designed and user friendly, accessible platform. The platform will have to provide the point of interaction between the two users type.
A friendly and easy to navigate platform can be of extreme importance to the investors, that would be more willing to trust it and invest in the ventures associated with it.

Payment:

Online secure and efficient payment activities are provided on the platforms to allow for a valid movement of capital between the parties.

Payment activities can be integrated inside the platform or can be provided by an external partner if necessary.

Banking:

Banking services are provided that include: access to credit information, account management counselling, and ex-ante financing.

Dunning & Debt Collection:

In order to protect users from any investment losses due to debt default, invoice and liability collection services need to be implemented.

These services are implemented in order to create a safer and more transparent environment for both capital-seekers and capital-givers.

2.3.3. Platform Interactions and Service Provisions

In the crowdfunding ecosystem, we can define different actors with different duties, necessary to support the network of services that is presented to the parties in this two-sided market. These services can be selected and divided according to their possible disruptive nature (Haas P., Blohm I., Peters C., Leimeister J. M., 2017). From the previous identification and modularization of services, we are able to select seven of them that according to Hass and al. can be provided by a general crowdfunding platform. Six of these seven can furthermore be considered disruptive in the market of capital financing. The different characteristics of the six services selected, allows us to divide them in two distinct categories; specifically, "crowd-related" and "funding-related". The distinction of these two categories will be helpful in explaining crowdfunding decentralized application's possibility to disrupt the current crowdfunding market in the near future.

The crowd-related category refers to the group of services to be implemented to satisfy the needs of the actors involved in the crowdfunding network. These services are also necessary in order to incentivize the interaction between the two major actors. These services are necessary for the existence of crowdfunding platforms.

Funding-related services on the other hand refer to the services provided by the external service providers in the market, that allow for the execution of funding actions, necessary for the creation of funding activities and the relative transfer of value and currency. The two categories can be thought as the creation of two levels of interaction between the parties around which the crowdfunding ecosystem is built, namely capital-givers and capital-seekers.

In order for the ecosystem to function, there is the need for three intermediaries to interact directly or indirectly with the parties. These "network partners" and their crucial role inside the system are represented in the figure below (Figure (12)) (Haas P., Blohm I., Peters C., Leimeister J. M., 2017).

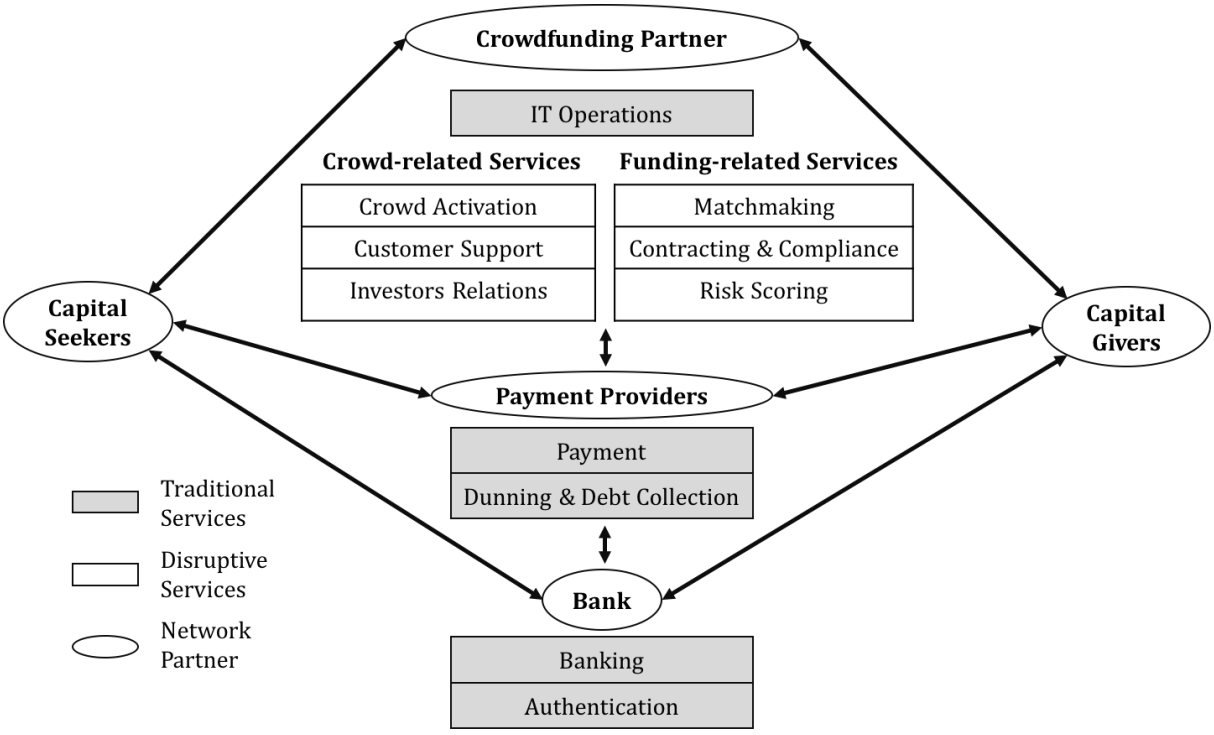


Figure (12): Network Partner Interaction in the crowdfunding system.

These are some of the most interesting services that can be provided by crowdfunding platforms. The Six services we have selected and divided in crowd-related and funding-related, are disruptive in the funding services environment. These services provide for a better communication and interaction between capital-seekers and capital-givers, reducing risk and uncertainty in the funding system.

The innovation brought by crowdfunding platforms has changed the world of funding and made it possible for many entrepreneurs to get access to funds and be able to construct strong and independent ventures.

2.4 The Growing Industry of Equity Crowdfunding

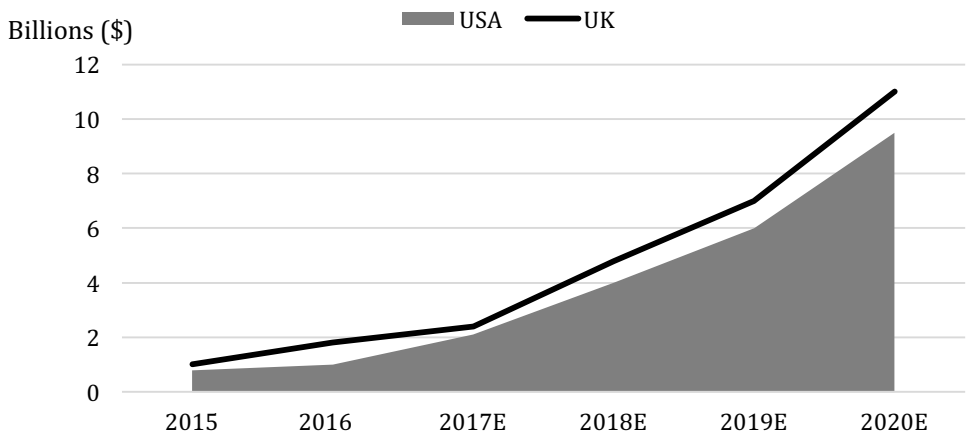
Despite the possible risks and the limitations of various platforms, the industry of Venture Capital that includes Equity Crowdfunding, have been growing substantially in past few years, becoming one of the major players in the financing industry.

In order to gather funds to enlarge and improve their businesses, small companies have very few options that would guarantee an access to funds and the consequent possibility to create a new venture.

The hesitation of banks in the last few years to lend money to entrepreneurs, has left the space for some other actors to impose themselves as major players in the field of financing new companies. Venture Capital was the first one to take control of the market; but Equity Crowdfunding is making its move fast inside the market, becoming one of the most popular methods (Greenhalgh H., 2016).

Equity Crowdfunding is one of the industries that is growing the fastest in the financing industry. Forecast say that the industry will raise about 11$ billions by 2020 (Kocianski S., 2016).

The graph below (Graph (1)) shows the increasing volume of capital that equity crowdfunding platforms are raising and will continue to raise given the forecast.



Source: Nesta, KPMG, BI INTELLIGENCE

Graph (1): Increasing volumes of capital raised by equity crowdfunding platforms.

Both investors and businesses are switching to this method of funding, because of the multiple benefits of the methodology. These benefits include the availability to anyone to participate even with small amount to the funding of companies that they believe have

the potential to be successful in their respective field.
The introduction of Equity Crowdfunding is leading to the consolidation of a trend in which the funding of new and established business, could be brought to the consumer market (Stengel G., 2014).
The traditional methods of venture capital, allow the participation to the market of only those that are willing to invest conspicuous sums of money. Venture Capital creates enormous entry barriers to everyone willing to face high risks, but with low liquidity availability.
Equity Crowdfunding on the other hand makes it easier for many willing to invest and undertake high financial risks, even if they do not dispose of substantial amounts of money.
On the other side of the market, start-ups and small companies that need financing, are able to have a bigger pool of possible investors from which they are able to get funds from.
The importance of crowdfunding in allowing the growth of small companies, is increasing fast and it is establishing stronger bases to become the next most used mean to raise capital.

2.4.1 Advantages with Respect to Venture Capital

Before crowdfunding came along, Venture Capital was about the only way in which companies were able to gather funds to start a business.
The use of the Venture Capital mechanisms can be in many cases of huge help for new ventures, and the expertise of the right Venture Capital company can really help start-ups to exploit their whole potential. For many companies, on the other hand, the use of this traditional method just does not fit with the owner ideas, expectations, and vision of the market. We have many examples of companies and funders whose idea and talent was not recognize by Venture Capitalists for many different reasons, including the fear of investing a conspicuous amount of money, in something that may appear too risky, unnecessary or not profitable enough for them.
There are many features of equity crowdfunding that might create advantages for this methodology with respect to the traditional Venture Capital ways. In this section we will analyse them and explain why Equity Crowdfunding might be the right choice for many new ventures and new entrepreneurs.

Easy Access:

Through the use of Equity Crowdfunding, the decision of giving capital to funders, does not come from one single individual, but from many inside the crowd. The access to capital is than easier and possible personal connections to investors are less relevant.

Equity Crowdfunding allows more investors willing to take the risk, to invest in new companies that they believe have the potential to create a sustainable entity. The amount of capital invested comes from a distributed network rather that given by a single Venture Capital firm, that would otherwise have to bear the entire risk by itself.

Venture Capital firms are usually composed by professionals in the evaluation of possible ventures. It is important to them to limit as much as possible the risk of the company when lending capital; so the idea presented to them must be interesting enough to allow for big financial investments, limiting the risk of failure for the project. The Equity Crowdfunding environment distributes the risk among many users, and tackles a larger share of the market, willing to invest in new and even more risky businesses.

Better Outcomes for Market Estimation:

According to Ethan R. Mollick (Mollick E. R., 2013), only 75% of companies funded through crowdfunding actually deliver the product they promised, letting down the investors that believed in them. Even so, Crowdfunding Ventures do get a better outcome for market estimation and the reason is not because of the type of projects or ideas that are proposed to the market.

Venture Capitalist have a great experience when it comes to starting a business and evaluation how said business will perform. When entrepreneur pitch their ideas, sometimes they do not have a clear view of the industry or the market in which they will have to compete. Venture Capitalist thanks to their expertise, are able to give a more precise evaluation of the idea, which is usually lower than the one that a less expert evaluator would give (Wilson K. E., Testoni M., 2014).

Equity Crowdfunding switches the power dynamic more in favour of the company that is been funded. The new venture will have to convince very few hundred people out of millions that participate to the crowdfunding activities, that their company is valuable and has the potential to reach all the goals that have been set.

We may have heard how some crowdfunding campaigns are unrealistically over valuated, but it is important to determine if these complaints are valid or have been pointed out by someone who is in need to protect their own business from disruption.

Better Financing Conditions:

Thought the traditional Venture Capital investment deals and contracts; Venture Capitalists are able to get most of their revenues. Using favourable investment conditions in the subscription of investment deals in fact, allows investors to profit substantially from their investment in new ventures, usually at the expenses of the entrepreneurs and their ideas.

With the use of crowdfunding, the power in contracting is given away from the Venture Capitalists and given to the entrepreneurs and to the crowdfunding platform. Equity Crowdfunding platforms are able to stipulate very different sorts of contracts that make it able for both the funders and the fundraisers to profit from the investment in new possibly profitable ventures. Conditions of the contracts are than not determined only by the venture Capitalists, but are determined by a combination of the different actors involved in the financing structure.

Visibility:

The level of awareness that can be reached with the use of Equity crowdfunding, goes beyond the traditional level of publicity that can be given by Venture Capitalist. The use of an internet platforms to publicize their product, gives entrepreneurs the chance to interact not only with a broad customer base; but also with a network of new suppliers, distributors, and other possible collaborating companies, that might add substantial value to their venture.

When a company is put on such a platform, the exposure can be used by the fundraiser to publicize its products as well as its vision and mission; being able to improve and enlarge its market and its network. The possible exposure given by these type of platforms can be of extreme importance for new ventures, whether the typical conversation with a Venture Capitalist is usually done through a protected and private conversation.

It is important to note on the other hand, that the public position a new venture takes, can be very risky in the case of failure. Failure on an Equity Crowdfunding platform would mean a public exposure of the failure, while on the other hand through a Venture Capitalist, the failed attempt to get funds would not leave the room.

Wider Investment Base:

Many of the companies that decide to upload their projects on an Equity Crowdfunding platform, have a "B to C" structure, and would benefit from an increase in the number of shareholders that might become successively, possible ambassadors.

Having a large number of advocates with the same interest and respond to the right incentives as the ones of the entrepreneur can be very valuable for a company that is still working on constructing a valid customer base.

As we will see in the next section[27] the use of Equity Crowdfunding has its limitations in giving the right amount of rights to shareholders and in protecting their interests once the crowdfunding campaign is over.

Does Not Eliminate the Idea of Having Collaborating Investors:

Crowdfunding is usually associated with the idea that the investors will not bring anything to the table besides their money. On the other hand, Venture Capital is usually associated with the fact that the experts associated with it, will be able to participate directly in the managerial activities of the companies using their experience to add not only capital, but their knowledge to the potential of the company itself. When faced with the decision whether to get the capital from one or the other systems, many fundraisers believe that the choice of using equity crowdfunding could result in the possible loss of possibly necessary knowledge. On the contrary, it is very plausible, and encouraged by Equity Crowdfunding platforms, that in the crowdfunding network there would be major funding investors that decide to contribute substantially to some projects, expecting to be involved in the board of said company.

Market Research Possibilities:

The creation of a new product to be presented to customers is the result of a continuous trial and error mechanism for the evaluation of what is mostly needed by consumers. There are different ways to make research in order to have the right information to develop a new product. Some companies are today turning to crowdfunding for the gathering of data for their market research.

[27] Section: 2.5. Inefficiencies.

The goal is to reach early adopters, willing to test on themselves the products and to give the company feedbacks on how to make to product better for more demanding future customers.
This method is mostly used by already established companies that are investing in innovation, but have not clear yet what customer requirements for such products are. The information that are gathered, become an important marketing and business tool in the development of the new product and the relative campaign.

2.5. Inefficiencies

As we have shown in the previous sections, the use of crowdfunding platforms is changing substantially the funding market, enabling funders to have access to small amounts to fund their organizations without going through banks or other traditional financial intermediaries. The crowdfunding system although, presents some inefficiencies and challenges that affect both sides of the market.
In this section, we will analyse the potential drawbacks and risks of using an equity-based crowdfunding platform from the point of view of the capital-givers.

Whenever we interact with an online platform or rely on an intermediary for the handling of capital or information, we need to keep in mind the possible consequences of using such third parties. Risks can arise in multiple forms, from the economic or microeconomic point of view, to direct platform related risks. We will further discuss these matters in the following paragraphs.

2.5.1. Microeconomic Challenges

When two parties are in the stage of development of a contract before a transaction, one of the two might have access to a list of information that might be more relevant than the information available to the other. The information not public to both parties, might be crucial for both in the determination of the conditions to be recorded in the contract. This asymmetry in the amount and validity of information available to the actors involved is referred to as “Information Asymmetry”. Information asymmetry may be considered one of the most challenging problems when dealing with equity-based platforms.
In the current state of the art of the crowdfunding system, mostly based on a reward system, the information asymmetry relies on the capabilities of the creator of the enterprise to develop or not the product that he or she promised to deliver. In the case of

equity crowdfunding, the information asymmetry involves not only the capabilities in producing a material product or a service, but also to the managerial and organizational skills of the entrepreneur. The creator of the possible venture in fact, must be able also to create a sustainable entity, with equity value able to work efficiently in the market.
The level of risk which funders face, is much higher considering that the creator will be required to create a structure made by a governance, reporting and accounting structure; all aspects of a company that are required to be maintained in a publicly traded market (Lerner J., Stern S., 2014).
We are able to divide the concept of information asymmetry in two independent but correlated issues when it comes to crowdfunding. These issues are "Hidden Information" and "Hidden Action". These complications affect the interaction that exists between agents through different stages of the process of raising capital. They have the potential to create market failure, limiting the possibility of the rising of value-creating transactions. Here below we present some of the consequences associated with information asymmetry and hidden information and actions, that can cause market failure (Lerner J., Stern S., 2014).

Adverse Selection:
The nature of these moderately regulated platforms, allows for the interaction between parties that could be even geographically far from one another. Low regulation and control, together with geographic distance on the other hand, could cause problems to arise in terms of information asymmetry. Funders in facts, due to such circumstances, may not be able to perform personally or efficiently a due diligence analysis before initiating a financial contribution to the projects in question. It could be hard for funders to access the accountability of the creators in creating a sustainable business in which they would be willing to invest.
On a web-based crowdfunding platforms this assessment is particularly difficult, and as a result, any project presented, may be discounted and underfunded, regardless of the value it might have on the long run. Consequently, high-quality proposals would not be put on the platform by creators, fearing a lower valuation of their venture and not achieve what could be considered as a fair price for their equity.
The bottom line result for this hidden information problem, is the participation of only low-quality ventures to the network of the platform. This "Adverse Selection", creates a

suboptimal equilibrium where high quality ventures funders and creators are left out from the opportunity of creating high standard transactions (Lewis G., 2009).

Moral Hazard:

The inequality in the distribution of power and knowledge, is not limited to the period of time preceding the investment actions. The issues related to imbalance of information and power in fact, arise also after the transaction went through and the funds are raised. The nature of the crowdfunding contract does not give any right to the funder over the actions of the creator after the funds are transferred.

The creator might change its approach to the market and to risk; acting in a selfish matter, and he might act not in compliance with what has been agreed upon before the investment went through (Lerner J., Stern S., 2014).

The structure of the system especially in an equity crowdfunding environment, does not also allow for the creation of a secondary market for the exchange of the investments. Meaning that once the campaign is over, the investors cannot sell their "shares" of the company they invested in, but it is all risk capital.

These hidden actions are the consequence of the "Moral Hazard" involved in these types of transactions (Bellaflamme P., Lambert T., 2016). As a consequence, funders may avoid using such platforms for investing, fearing possible mismanagement of the capital invested; this would result in a market failure and the shutting down of the platform.

Principal-Agent Problem:

One of the most common examples of a negative consequence arising from the Hidden Information and Hidden Actions issues, is the "Principal-Agent Problem". This problem arises when the actions of the creators are not in line with the interest of the funder. These actions may be the result of business information related to the insider position the funder has in the market; or more simply, the not alignment of the interest of the two parties involved.

The absence of a secondary market for investments, limits the actions of the investors in the case in which the actions of the fundraiser are not in line anymore with their interests. The system does not allow for a back out option after the campaign is over.

The Principal-Agent Problem is a common consequence of the miscommunication that usually occurs between funders and fundraisers. The communication system inside the

platform should be constructed such that objectives of both actors are clear before and after the initialization of the first transaction.

Collective Actions:

Due to the information asymmetry present in such platforms, one of the issues that might arise is the "Free Riding" problem. Investment information inside the platform are public, meaning that some funders may rely on others work in the definition of a solid due diligence. Funders inside the platform in fact, in order to avoid the issues listed above, might rely on the decisions made by other peers, slowing down the fundraising process. If this would be the case for every funder present on the platform, the market would stop and eventually fail, since everyone would be waiting on others to make the first move (Lerner J., Stern S., 2014).

Information Asymmetry cannot be managed completely by the crowdfunding platform. The power and the resources of the platform, are usually limited to its boundaries; and it can be difficult for the platform to offer a precise and deep analysis of the fundraisers once they create a new campaign. The analysis could include the financial and credit record of entrepreneurs. From the point of view of funders, having access to this type of information would mean have access to a complete view of the person they are asked to trust, making the trusting procedure a lot easier.

Same goes for funders; having the right information about possible fundraisers may help them to select the right crowd to fund their project, making the crowdfunding procedure a lot faster and easier.

2.5.2. Risks Associated with Crowdfunding

There are five major financial risks related to a crowdfunding platform for the agents involved. We can evaluate the possible challenges by analysing a series of different risks related to them; specifically: Risk of Default, Risk of Platform Closure, Risk of Fraud, Liquidity Risk, and Risk of Cyber-Attack (Kirby E., Worner S., 2014).

Even if we will not discuss about them, it is important to take into consideration also the risks associated with innovation in the open market, that include: Investment Risk, Development Risk, Co-Ordination Risk, Motivation Risk, Control Risk, Security Risk, Governance Risk, and Culture Risk (Amalar L, 2010).

Agent risk of such sort may lead to risk of default or fraud, and unfortunately crowdfunding intermediaries do not currently offer tools to attenuate these specific agent risks, exposing dangerous agents participating in the network.
One of the services in which platforms invest substantial resources, is the screening of possible businesses before the presentation to the public of investors. These screening processes are created in order to allow funders to have as much information as possible when making financial investment decisions, and offering appropriate and secure projects. These percussions are in fact necessary in such circumstances to avoid the issues previously presented. The presence of such attention and sagacity by platforms increases their prestige, but exposes them to different types of risks, such as cyber-attacks.

As we earlier said, open innovation related to crowdfunding leads to certain problems conducing to the issue of Moral Hazard and the Principal-Agent issue. Unfortunately, inside a crowdfunding platform, this requires an extra effort by funders in screening the activities of the creators. The information they need to gather, are related to both, the project that is been presented to them, and the historic financial and credit behaviour of the creator of the project. These research and analysis are time consuming as consequently costly to the funders, that as a consequence will be recompensed more in terms of interests on the capital they decide to lend.

Risk of Liquidity must be mentioned and kept is strong consideration when talking about risks associated with crowdfunding platforms, since it is one of the most relevant risks associated with these activities.
Once the investment is done, and the campaign is over in fact, funders have no option but to remain partners of the company until the unfolding of the market. It does not in fact exist an outside and secondary market on which obligations of this type could be managed, sold or bought after the creation of the venture. This limits the actions of the funders making them face really uncomfortable financial investment decisions, with very little information about the creator at their disposal. This high level of uncertainty leads to an abandonment of platforms by funders and to a lowering of the position of the phenomenon of crowdfunding.
The Liquidity Risk issue has very strong implication in the crowdfunding market, that may result in the creation of a closed market, limiting the entrance to the actors that are willing to face high risks and uncertainty. The absence of a secondary market and the localized

regulatory rules, like specific national laws, about crowdfunding and similar networks; might also lead to the creation of closed and confined webs of investors and creators, that hardly connect with one another. The name of the risk associated with this phenomenon of separation of the networks is “Systemic Risk” (Kirby E., Worner S., 2014), and is associated with the limitations that the creation of national regulations imposes to the openness of the market.

CHAPTER III

Crowdfunding Integrated in a Blockchain-Based Ecosystem: Decentralized Applications (DApps)

In the previous chapter, we analysed the different types of inefficiencies that a crowdsourcing platform may present for the parties involved, meaning capital-seekers and capital-givers. In Chapter I on the other hand, we introduced a new type of technology that could change the rules of the game for many industries and at the same time allow for the creation of new ones. The introduction of the concept of blockchain and tokenization, together with the decentralization of managerial and financial activates, may create favourable situations in which some of the previously defined inefficiencies of traditional equity crowdfunding could be mitigated.
In this Chapter we will also see what the challenges arising from the introduction of this technology might be, together with the possible future development of the technology that has the potential to disrupt the industry.

From what we have seen in Chapter II, we can state that a crowdfunding intermediary plays two major functions in the environment. The first major function played by the crowdfunding platform is the mechanism of creating a bridge of communication and interaction between the two major parties involved in crowdfunding business. The second crucial function is the creation of a structure, that enables the rightful transaction of funds between the two parties.
The platform, following these two major functions is able to implement a list of tools and services, in order to make the platform better, more secure, and easy to use for the users. Thought the descriptions we will provide of the platform and the services, we will make a clear distinction between tools, underlining the reasons that led to its implementation and to which major function they are linked.
We will focus on one of the major functions that a crowdfunding platform performs in the sustainment of the ecosystem. The focus on this chapter will be on the mechanisms that regulate the funding processes of the equity crowdfunding platform. We decided to follow this path since, it is in this field in which blockchain technology can come in handy.
We will see how the technology allows for the creation of the so called “Decentralized

Application" (Dapp) and how it can be adapted to the crowdfunding environment to help create a Blockchain-based Crowdfunding Platform, that can be able to satisfy many of the needs of current crowdfunding clients, and resolve many of the issues related to the traditional methods of crowdfunding.
DApps have the potential to resolve many of the problems associated with the current state of the art of crowdfunding, and allow for new and better mechanisms for the protection of both funders and fundraisers.

3.1. Functionality, Structure and Design of a Crowdfunding DApp

One of the most important innovation brought by the introduction of blockchain technology is the introduction of a crowdfunding DApp. The crowdfunding DApp allows for the integration in the system of many new functionalities, and creates a bridge between the users and the blockchain technology and its potential.

In order to perform certain functions in a standardized and computerized way, Smart Contracts are used to administer the functions built inside the Crowdfunding Decentralized Application.
A deep look into the functionalities offered by the DApp backed by the technology and logics behind smart contracts, will help us understand all the applications and the functionalities that a DApp is able to offer, and the necessities it is able to satisfy.
The Crowdfunding DApp is the bridge between the users and the blockchain; is the holder of the programs that regulate the new functions.
In section 1.5.3, we gave an explanation on the functions and structure of smart contracts, on how they can be constructed and are built. That explanation about smart contracts is necessary to understand how they have the potential to be implemented in an equity crowdfunding environment, to help ameliorate many of the different services that are usually provided by a traditional crowdfunding platform.
The structure of the smart contracts that we will further analyse, refers specifically to the all-purpose framework that is offered by environments like the one of Ethereum. Ethereum, like many others, is in fact able to offer developers and companies the possibility to enter in the network with a smart contract, in many different ways regardless of the industry in which they are working in. The flexibility of the Ethereum network can allow the integration of transparent and customizable protocols, with a set of generally delineated smart contracts. This is able to to make the network safe, secure,

immutable, and decentralized; though dependent by the decisions of the final users that are the principal contributors to the equity and liquidity of the network.
In this section we will see many of the functionalities, the structure and the design of a crowdfunding DApp. We will do so in order to understand in depth how these applications are constructed, why they are constructed that way and what is the level on interaction between the actors inside the network and the DApp.

3.1.1. Functions Performed by the DApp

It is important to define first, five of the most important functionalities that a crowdfunding DApp can offer to both sides of the system, meaning capital-seekers and capital-givers.
The mechanisms explained below, give a detailed vision of the structure of a crowdfunding DApp, and how the interaction with the main platform is performed. We will be able to see the differences between the common functionalities offered by a traditional crowdfunding platform, and the ones offered by a blockchain-based crowdfunding DApp.
For the sake of clarity, it is important to point out, that in a blockchain-based environment, whenever we talk about funds, we refer to an amount that can be given in the form of cryptocurrency or in fiat currency[28]. The decision on whether to raise capital in crypto or in fiat, depends on the necessities and the preferences of the funders during the crowdfunding campaign. The decision to allow both, makes it easier for investors that are able to decide to invest with whatever currency they prefer.

Smart Property Tokens:

The capital-givers are investing in companies in an equity crowdfunding environment, this means that they are buying a portion of the company they are investing in. In order to prove the ownership of the section the company, or a simple proof of the investment, they receive "Smart Property Tokens" from the DApp they invest in. Tokens represent a portion of the company, and their price is determined by the fundraisers. The price of tokens is based on what fundraisers believe the company potential is, and on how much value they want to gather in order to make the company grow.

[28] **Fiat currency:** Fiat currency is money without intrinsic value. The value of fiat currency is determined by government regulations. It can be considered of value, only because the government uses its power to enforce the value of that currency.

Each project or entity, is able to issue its own tokens, that are linked to the project that is been developed. The ownership of the tokens creates a binding relationship between the funder and the company, entitling the capital-giver to certain rights associated to the property of that given token.

Tokens can be considered as holders of value, similar to the concept of shares of a company, whose value is determined by the fundraiser at first, but can increase or decrease depending on the rules of the open market for tokens.

At the beginning of the campaign, the fundraisers set the name and the initial value of the token they are willing to issue, dependent also on the amount they want to raise. Smart tokens are issued every time a contribution to the crowdfunded campaign is done.

Precise rules regulate the degree and level of rights and power that are to be granted to the funders at the end of the crowdfunding campaign, where the company will use the funds acquired to build the project as they promised. The enforcement of those rights is not given to a centralized authority, but to the software that regulates the relations between the two parties. As we know in fact, the smart contract is in charge of applying the rules, and will execute always as soon as certain requirements are met.

Every token in order to be linked to certain rights, is in possession of its personal private key. The owner or holder of the private key related to the token, is consequently the owner of the token itself.

Trading of keys and tokens is allowed in a blockchain-based environment. this is of particular importance, since it allows for the creation of a secondary market for tokens. The secondary market allows for the exchange of tokens between investors, solving one of the biggest problems for the traditional crowdfunding environment. We will take a deeper look into the potential of the secondary market for tokens in section 3.4.2 of this Chapter.

Tokens can be considered to be valid as long as the company to which they are associated is running. In the crowdfunding phase, tokens maintain a steady value set before the beginning of the campaign; as soon as the campaign is over, the value of the tokens varies depending on the performance of the company and of the rules of the market.

If the campaign fails because of the reaching of the time limit to raise funds, the tokens become valueless and the amount of the investment is given back to the owners of the tokens that invested in the failed campaign.

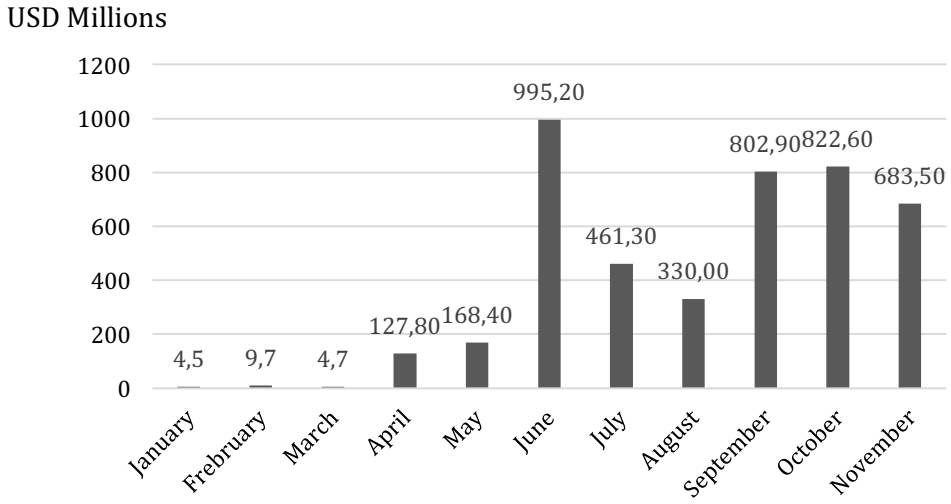
If the campaign goes through, the tokens can be exchanged and the price can fluctuate depending on how the market is responding to the company, and on how the company is

performing.

The first issuing of smart tokens by a company and the initial determination of the price of those tokens, is called the ICO or “Initial Coin Offering”. The ICO is the first token sale or launch in the market for tokens.

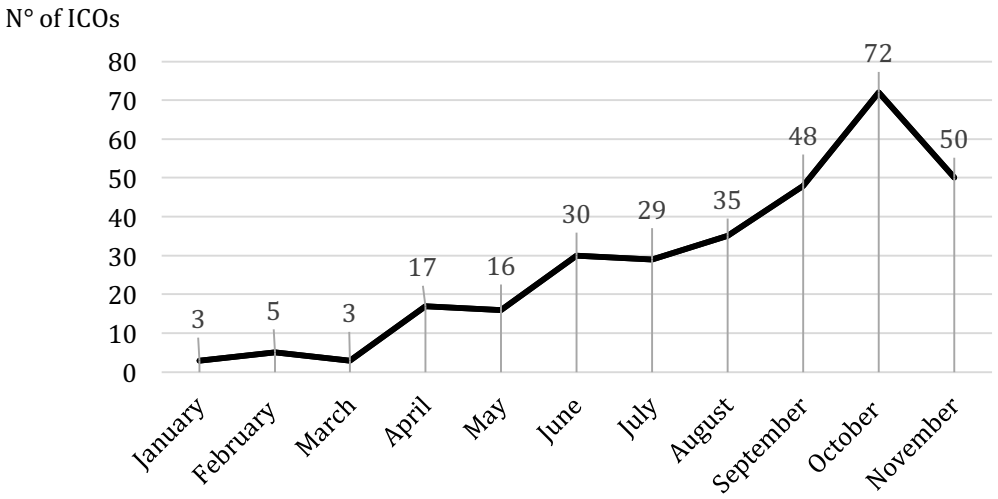
The token sale helps the company to raise money by selling shares of itself to a network of partners. This can be done even outside a crowdfunding platform, and it is used like the traditional selling of shares in the public market. It is similar in fact, to the traditional IPO concept, in which companies decide to become public and sell a given amount of shares to raise capital for new projects or when in need of liquidity. They are in fact an alternative to the the traditional Capital-Funding of Venture Capitalists and Equity firms.

2017 has been the year in which the industry of ICOs has boomed extremely rapidly. The data shows how the amount of funds collected by ICOs, has reached an astonishing 4,4106 USD billions in just 2017 alone. In July 2017, the average collected funds for an ICO, was of 33.17 USD millions. The graphs below (Graph (2) & Graph (3)), shows graphically what has been just explained.



Source: Coinspeaker, 2017

Graph (2): Capital raised by ICOs in USD Millions during 2017.



Source: Coinspeaker, 2017

Graph (3): Growing N° of ICOs in 2017.

In November 2017, we have the ICOs that raised singularly the greatest amounts yet. QASH (Trading & Investing company) is leading the group with a 108,2 USD millions raised in only four days, followed by WAX (68,4 USD millions) and Gridplus (45,7 USD millions). Switzerland is the the nations that is currently more active in the creation of ICOs; 4 out of 6 ICOs in fact come from this country, thanks to its favourable business oriented and innovation oriented legislations (Dr. Diemers D., 2017). We will go deeper in this discussion in Chapter IV.

The biggest difference from the traditional methods of raising capital, relies in the fact that through this technology, also new and small start-ups can have access to similar financing tool; without the need to rely on traditional business angels, venture capitalists or banks in order to raise funds.

Crowdfunding Campaign:

Before we begin to define the differences in the mechanisms related to the new system to raise capital, it is important to note that the introduction of the technology does not necessarily make it harder for users to interact whit the platform. The front end of the platform, meaning the interaction with the crowdfunding platform by users, is very similar to the traditional methodology of crowdfunding. The new technology stays in the background and does not increase the difficulty with which interactions are made inside the platform, but simply helps improve the quality of the services provided.

One of the first elements that require the interaction with the system, is the crowdfunding

campaign. There are several stages that lead to the success of a campaign, and they depend on the achievement of certain steps. They especially depend on the achievement of the objectives set before and during the campaign and in the end on the accomplishment of the financing objective.

One of the first major differences brought by the blockchain technology, is the structure and the mechanisms engaged for the raising of capital.

The funds given by the funders are not directly transferred to the creators, but they are stored in a separated account, where they will remain locked until the funding goal is reached, or the deadline for the collection of the funds has passed. If the case occurs in which the thresholds are not reached, the smart contract inside the DApp is coded in such a way, that would release the funds back to the funders; that will be able to invest them in another, more profitable project. If on the other hand the funding process has a positive outcome, the smart contract that manages the funds, will move to the next step of the crowdfunding procedure. This procedure consists in attributing the pre-determined rights to both the owner of the tokens and the fundraisers, and unlocking the funds raised so that they can be used, under certain rules, by the fundraisers.

In this phase, through the use of digital signatures, funders and fundraisers related to the project can use their rights to perform actions on the funds linked to the project. These rights allow both the funders and the fundraisers to have a certain control over the funds and make possible actions and proposals to use them. We will see in next few paragraphs what these rights are and how important they are for the creation of a decentralized, transparent and safe environment.

In the early stages of the campaign, rules need to be defined with respect to the rights and power that each actor wants to achieve or have during the development of the project. It is of extreme importance to have a clear definition of the rights and the obligation of the actors involved, in order to avoid future issues related to power and decision making. The funders for example would need to set, make public and have certain rights on the amount they intend to invest, while on the other hand, fundraisers would want to have full control over the raised funds. Inside the smart contract, that defines each one's rights, these rules are written down and become inviolable once anyone decides to participate to the project.

Decentralized Autonomous Organization (DAO):

A "DAO" or "Decentralized Autonomous Organization" has similar functionalities of an investment fund, but integrated in a blockchain-based environment. Instead of directly

investing in new ventures, funders may decide to invest first in a DAO, and wait for new projects to be proposed to it. Once projects are proposed to the DAO, their voting power makes them able to decide whether the money they invested should go to that specific project or not.

Being members of a DAO, allows users to propose ideas to the rest of the internal network, and invest in some of the projects proposed by other members. A DAO does not create physical products, it does not develop soft or hard ware; on the other hand, it is able to receive and present to its token holders, different investment proposals. In order to do so, it requires a "Contractor", which can be any DAO token holder that makes a proposal to the DAO; this proposal can be accepted or rejected by other DAO token holders.

Note that trough this system, the token holders have the chance to make the DAO grow, by creating contracts or proposals to other token holders, that will make the DAO grow and gain more funds.

The rewards for investing currency in the DAO are indeed DAO tokens registered in the name of the account that invested in the fund. A token empowers its owner to have claims over the company, meaning that the investor will gain voting power and other right as an associate of the DAO.

Like shares of any other traditional company, the number of tokens received is relative to the value invested. Price for tokens follows the normal market rules of demand and offer, and are easily transferable inside and outside of the DAO.

Proposals can be done directly to the DAO and propose a certain use of the funds stored inside it. Whenever a proposal is done to the DAO for a new project, the initial quorum for a traditional voting is 20%. In the case in which the amount requested by the proposal, would be the totality of the value a DAO has accumulated, the quorum necessary to make the proposal pass would be of 53.33% of the token holders (Jentzsch C., 2016).

To avoid receiving an excessive number of proposals, a proposal fee (changeable with a proposal) is required. If the quorum is achieved, the total amount for the fee is refunded to the contractor; if on the contrary it is not achieved, the deposit is kept by the DAO.

The proposals have an expiring date, at the end of which, if the goal is not reached, all the currency accumulated is returned to the contributors, and the total amount of tokens created are eliminated.

If the proposal is accepted, the DAO transfers the necessary currency in the Smart Contracts that represents the proposition; and by doing so, it starts a new project.

Once the new venture is up and running, decisional power of users is directly correlated

to the number of tokens they possess. Tokens are divisible in fractions, transferable in the secondary market, and identical.
Once the contract is established, whenever the contractor makes a proposal, users can vote on it during a defined time slot. When the voting window is closed, a request can be filed by any token holder to certify that the the majority and the quorum necessary to make a decision has been attained.
In order for a new decision about the project to go through, the majority of the token holders or at least a minimum amount of them, must agree on the new proposal. The level of the quorum can vary, and can be changed with a proposal. The quorum depends on the number of participants, the number of tokens issued, the value of currency used to create tokens, and the total amount that the project has accumulated.
The DAO complexity can vary depending on the role it is given to, and the number of signatures, or conditions it needs to function. This means that the number and the level of interaction between the parties varies depending on the conditions that are determined to be part of the DAO.

Decentralized Autonomous Organizations can play an important role inside a blockchain-based crowdfunding environment. The use of the DAO can provide an easier way for the protection of investors to come in contact with innovative projects and invest in these profitable new ventures.
What makes the DAO work, is a line of code, and just like a smart contract, it is developed using the Solidity programming language. In order to work, a DAO needs to be uploaded on a blockchain that supports it. Once on the network, it will perform many function in the managing of funds, rights and permissions, as well as the production, management, and verification of transactions.
When a DAO is utilized in a crowdfunding environment, it covers one of the key roles in the design of the environment. The DAO plays two major roles: the role of the holder of rights for users offered by the DApp, and the role of holding the funds while any projects is being funded. When developing the code of the DAO, particular attention needs to be put in the functionalities embodied in it, and the rights it will allow once the project has taken off. Rights and obligations of the two actors need to be clarified and specified deeply; once the program has started, it becomes very difficult to interrupt the cycle.
A DAO is able to communicate, if necessary, with other contracts inside the network. This allows for a wide level of possibilities and functionalities across the network, in which

automation of actives will substitute many of the currently commonly used applications. The potential of the DAO is enormous, given the fact that it represents completely the will of the owners or shareholders; technically allowing it to grow and evolve and communicate with other DAOs to create an even bigger decentralized network.

Voting System:

One of the major difference with the traditional environment, is the allocation of rights among users. The new technology allows for a stronger allocation of rights to funders, that allows for a decentralization of decision making that could disrupt the industry.

Before the issuing of tokens, the fundraisers set the limit of the rights to be given to token holders. Every token can be associated to the ability of a token holder to express one single vote, whenever the right to vote can be expressed in a decision making situation.

Whenever a new proposal is issued by fundraisers, a vote can be used to allow the generation of different actions, such as spending of cryptocurrency, interaction with different or external contracts, or even the elimination of another proposal. The execution of the proposal that has been validated by the voting actions, will be executed as soon as it reaches a majority.

As explained before, the right associated with the holding of tokens, like voting rights, are defined by the creators of the campaign before the proposal becomes public.

Voting rights democratized deeply the environment; rights and power are put back in the hands of final users.

Withdraw Tracking System:

When designing the DAO and its powers before the deployment of a project, the fundraiser is able to create not just the rules that regulate voting rights, but also rules that limit the withdraw from the funds raised. What it means is that there can be rules embodied in the DAO code, that limit the amount of the funds that can be spent by the fundraiser in a given delta of time. These rules are created in order to protect the interests of the funders, which are also entitled to decide on how that money can be spent. It is important to remember also, that the nature of the blockchain technology, makes every transaction public to all the members of the network; meaning that all the movement of currency or the possible investments made by the fundraisers, can be monitored and through the use of voting rights, also be blocked.

Once the threshold set by the partners is surpassed, any transaction that requires access

to the funds will not be allowed. If the funders require necessarily that amount, what they can do is create a proposal, on which funders can vote weather to allow for the spending of the extra money or not.

3.1.2. Equinity Crowdfunding DApp Relational Structure in the Network

We now have a clearer vision on how the traditional crowdfunding platform can be changed by the introduction of blockchain technology. We now also have a clearer definition of some of the new actors that would compose a blockchain-based equity crowdfunding environment.

In the Figure below (Figure (13)) the representation of the relationship between the two parties and the equity crowdfunding DApp is shown. In the figure is is shown also the role of the DAO and the services that are embodied inside it. These services embodied in the DAO are the ones highlighted in a darker tone.

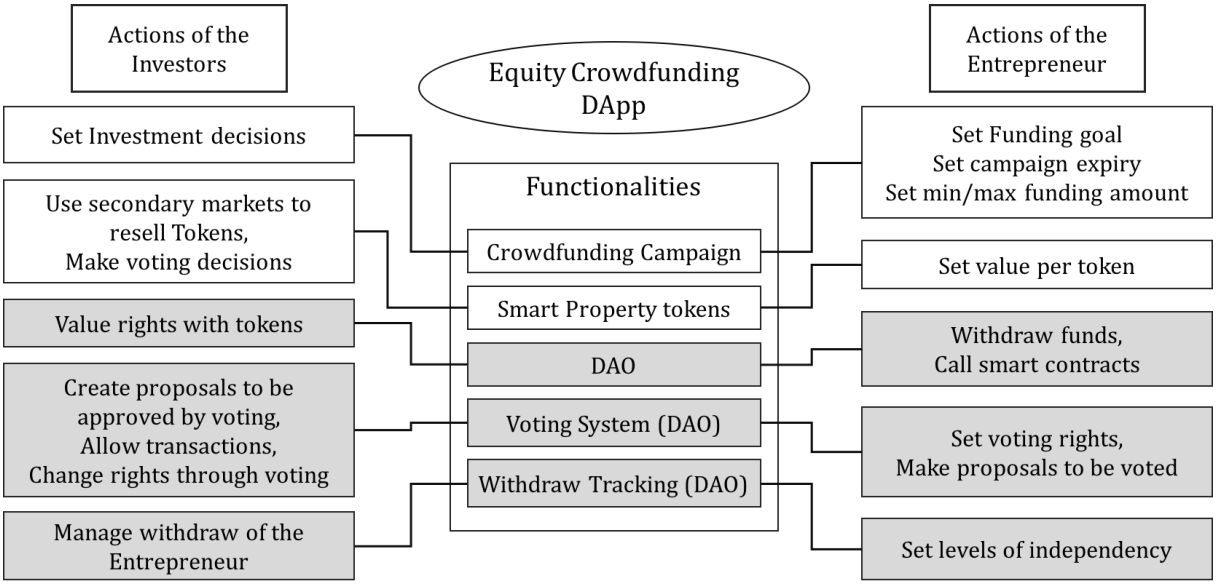


Figure (13): Relationship between the two parties involved and the DApp and its DAO, in the equity crowdfunding blockchain-based ecosystem.

From the figure we can clearly see the obligations and the rights associated with each actor, and how the Equity Crowdfunding DApp plays the role of the intermediary creating an information and relational bridge between the two.

It is important to remember though, that even if the DApp is actually playing the role of the intermediary, it is itself does not operate any control over neither of the actors in the environment. The major role of the equity crowdfunding DApp is to improve the level of

communication between the parties in the market, and allow them to collaborate in a more secure, safe and transparent environment.

3.1.3. Services and Functions

As we have seen so far, there are differences in the structure of a blockchain-based equity crowdfunding platform with respect to a traditional equity crowdfunding platform. We have also seen what are the new functionalities that an Equity Crowdfunding Decentralized Application might have and what effect it will have on the protection of the rights of users in the network

In the following section we will associate the traditional services that can be provided by a traditional equity crowdfunding platform, with the functionalities that these new decentralized equity crowdfunding applications can have constructed inside them. This way we can see how the new functionalities are related to the different services that are notoriously necessary for normal users inside a crowdfunding network.

In order to be as clear as possible, the table below (Table (2)) shows the connection between the traditional services, and some of the new functionalities associated with a decentralized application in a blockchain-based equity crowdfunding ecosystem.

Functionalities	**Services**
Crowdfunding Campaign	Matching, Payments, Banking, Dunning & Debt Collection
Smart Property Tokens	Investor Relation
DAO	Investor Relation, Payment, Banking, Dunning & Debt Collection
Voting System (DAO)	Investor Relation
Withdraw Tracking (DAO)	Investor Relation
Risk-Scoring System	Risk Scoring
Smart Identity Authentication	Authentication
Crowdfunding Application	Contracting & Compliance, IT Operations

Table (2): Functionalities of an equity crowdfunding DApp associated with the services provided and necessary.

As we can see, the services highlighted with a darker colour, are associated with functionalities that are not present in the traditional equity crowdfunding ecosystem.

The use of this new technology and innovation is able to create new functions, that are able to satisfy the same needs of customers, but with substantial improvements.

Major improvements brought by the new structure, are related to the Investor Relationship side; given by the introduction of functionalities such as smart property tokens, and the use of a Decentralized Autonomous Organization.
DAOs introduction allow for many advantages in the field; advantages that include the voting system and the withdraw tracking system, which empower investors in ways that were hardy implemented before. Investor Relationship improvement is what really drives the advantages of the introduction of this technology. With the idea behind blockchain, we can have an empowerment of the people that support the platform; we can create a safer environment where the investors feel at ease in the act of investing in new businesses and innovative ideas.

3.2. Blockchain-Based Equity Crowdfunding Environments: Business and Interaction Models

Now that we have a clear vision of all the functionalities of a blockchain-based equity crowdfunding DApp, we can analyse how the introduction of blockchain technology and the DApp can change the interaction models inside the crowdfunding environment.

The relationship between the two major actors and the third party will change, and in order to understand better the level of interaction and the role of each party involved, we present two different interaction mechanisms to explain transaction flow in this network in which a blockchain-based equity crowdfunding DApp is utilized.
It is fascinating how the level of independency from a third party of the two agents, is much higher in a system in which the blockchain technology is utilized.
In a traditional system, the interventions of third trusted parties like a bank and a crowdfunding platform are necessary. In the traditional ecosystem, the absence of these intermediaries would not allow for the development of services like banking and payments, necessary for the financial and communicational needs of creators and funders in the network.
As we will see, the role and the position of these intermediaries will change with the introduction of blockchain technology. The technology eliminates some of the traditional intermediaries and will simplify the network, by establishing a more direct communication, easier and more transparent interaction, and fair distribution of relevant information, solving many of the issues related to the traditional methods of equity crowdfunding.

On the plus side, the role of managing the allocation and distribution of funds, is no longer responsibility of the traditionally used crowdfunding platform itself or of a financial intermediary, but it is managed differently by the crowdfunding DApp and the related DAO; both decentralized and constructed to allow a higher level of transparency in the interactions between the capital-seekers and capital-givers.

The introduction of a Decentralized Application, has a strong effect on the traditional structure of the crowdfunding network. In Chapter II we explained two important contribution network structures, the "Peer-to-Peer Contribution Mechanism", and the "Equity-Based Contribution Mechanism". In the next two sections we will see how the introduction of the blockchain technology has an effect on the structure of the network, and how the DApp will come into play.

3.2.1. Peer-to-Peer Contribution Mechanism Trough a Decentralized Application

In the peer-to-peer contribution mechanism, where blockchain technology is introduced, the major difference with the traditional method lies in the holder of the mechanism that controls the flow of funds and the flow of rights. This role of the holder of such mechanism, is in fact played by the DAO inside the Crowdfunding DApp, of central importance in the network.

As we can see, the use of the DApp allows for a resolution of the problem of transfer of rights of the shares between the creator and the funder. This means that there is the possibility for the creation of a secondary market, in which rights on tokens can be exchanges, resolving one of the major problems related to traditional crowdfunding platforms.

Through this method furthermore, the DApp carries out the role of the holder of the funds devoted to the creator. This means that funds are not directly and immediately transferred to the entrepreneur, but are hold by the DApp. This allows the creation of systems in which access to the fund by the creator is managed by certain rules in the hands of those that are holding right of the company. This empowers right holders in a way that was not possible through traditional methods of crowdfunding.

The figure below (Figure (14)) shows how the structure of the peer-to-peer contribution mechanism changes as the blockchain technology and the DApp are introduced in the network.

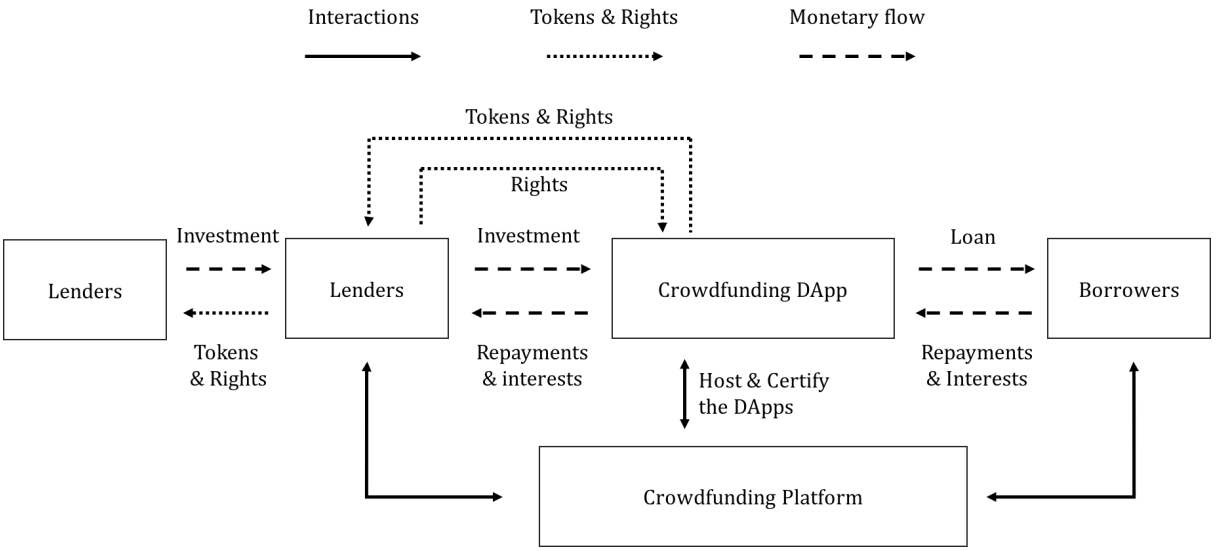


Figure (14): Peer-to-Peer Contribution Mechanism trough a decentralized application Illustration.

It is important to note how financial institutions like banks have no role in this system; and how the interaction of the lenders is not limited to the ones they can have with the platform, but extend to other lenders too.

3.2.2. Equity-Based or Royalty-Based Contribution Mechanism Trough a Decentralized Application

Similar structure can be found in the equity-based contribution mechanism structure; where entrepreneurs and investors can interact with each other directly. Also in this system, financial institutions like banks have no role, and can be eliminated; trust than shifts from financial institutions, to the technology itself.

Figure (15) shows how the the structure of the network changes for an equity-based contribution mechanism, when the blockchain technology is introduced.

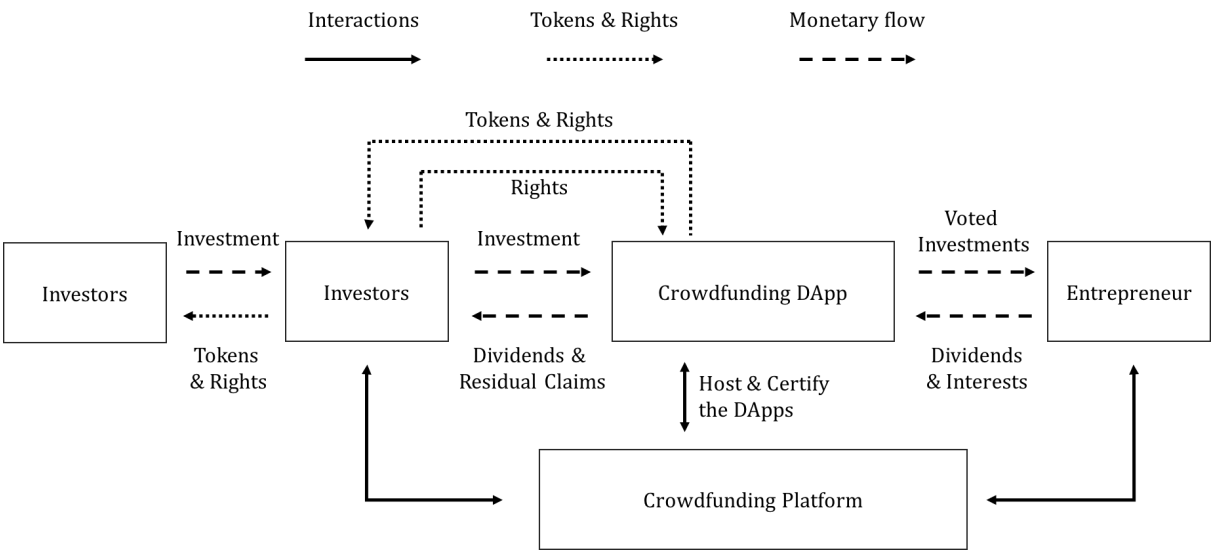


Figure (15): Equity Crowdfunding Mechanism trough a decentralized application Illustration.

As we can see from the figure above, the equity based mechanism through a decentralized application is very similar to the peer-to-peer interaction trough a decentralized application. As we know in fact, the introduction of decentralized application that works on a blockchain base, will allow for the creation of a peer-to-peer communication and financial interaction.

The left side of the illustration, shows the possible interaction between different investors, and the possibility for the creation of a secondary market for tokens.

3.3. Service Modules for Crowdfunding in a Blockchain-Based Ecosystem

The introduction of a blockchain based system in the crowdfunding model, has effects on many aspects of the industry. The technology has the chance to change also the approach to certain issues present in platforms of this type. Blockchain technology is in fact not only introduced to resolve many of the issues that we faced with the traditional crowdfunding mechanisms; but it is also able to transform some of the services previously provided.

In the Chapter II, we analysed some of the services that a traditional financial intermediary and a crowdfunding platform can offer to users; in this section we will explain how blockchain technology can improve some of these services.

Not all the services can be improved through the use of blockchain; we will focus only on those that can support a blockchain application and that can actually be improved by the technology.

Once we have identified the services improvable by a blockchain technology, we can

implement them inside a specifically designed DApp.

3.3.1. Service Modules Implemented with Blockchain Technology

Starting from a blockchain-based environment, we can take some of the traditional crowdfunding services and tailor them in order to fit the new system. We start from the definition and division of services provided by the technique of modularization of services that we analysed in Chapter II. We than describe the evolution of the services, reconfigured in the Decentralized Crowdfunding Application. What we know from the definition of the technology, is that the evolution of the services in the new ecosystem will be able to offer the same type of services, but with a higher level of security, transparency, and a lower risk for all the parties involved.

Matchmaking:

This specific service has no particular difference from the traditional form of matchmaking.

The main difference is the scope of the customer base in which the platform will operate. With the reduction of the minimum amount of capital necessary in order to fund a new venture, the market will tackle a section of the market until now untouched. The focus will in fact shift to the mass market, in which many individuals are willing to invest in risky new ventures even if they are not in possession of a great capital. What can also be developed is a more precise search mechanism, that allows for a partial or null publication of personal data, but is able to search according to a selected interest or to a selected level of reputation.

Contracting & Compliance:

One of the most important and interesting aspects of DApps, is the fact that the contracting and legal bureaucracy related to crowdfunding or any financial service that a platform may provide; can be managed automatically trough smart contracts. Costs related to legal correspondence and security, can be decreased substantially allowing for the allocation of resources on different services.

Customer Support:

The protocols that exist inside a Decentralized Application has the major characteristic of being clear-cut and computerized; this means that a full covered support is not needed to

interact with it. One problem can still arise from the stipulation of the digital contract, and in the understanding by the final user of the code that composes the contract. This problem is easily overstepped through a thorough explanation of the code embodied in the smart contract, in the same way it would be overstepped through the traditional methods.

Risk Scoring:

Due diligence analysis would still be performed by experts in the field, since the analysis of the feasibility of a projects can hardly be automatized. What the technology can do on the other hand is the analysis of all the past transactions of the fundraisers, in order to access their financial eligibility.

Instead of being performed by an external third party that has access or holds sensible private information about the users; this function could be performed by a smart contract. The smart contract could be able in fact to assign a score associated with risk to each individual by going through the transactions associated with said user. Since an automated cryptographic system is in charge of the analysis of the data, there is a reduction of the risk of having lower security. These controls could be performed through a smart contract embodied in the application proposing the project or, by a secondary contract that has the only purpose of associating each user to a risk score.

Authentication Through Smart Identity:

The application of Blockchain technology gives the possibility to any platform, to use Smart Identity applications. The technology allows for a more secure and precise authentication system that can be integrated in the central DApp or outsourced to another Decentralized satellite application.

This is of extreme importance in the definition of the identity of the funders and the fundraisers; not just for fiscal purposes, but especially for security and transparency purposes.

Crowd Activation:

The application of Blockchain technology does not affect the upfront services that a platform provides to users. Crowd activation services remain outside of the scope of a DApp, whose primary activities will be performed in the background, offering a more secure, and transparent way to transfer funds and data.

Investor Relations:

Investor Relationship is substantially improved by the introduction of this technology in the network for many reasons.

Unfortunately, regulation related to equity investment is for now inexistent or very limited for the use of tokens for crowdfunding investments, but the newness of the technology is giving space for the deep exploration of the possibilities of the technology; allowing for different, innovative and smart ways for supplying shares.

This system is able to give voting power to token holders, meaning that they are entitled of deciding how and when the money they invested should be spent for further projects. The transparency allowed by the technology also has the power to give rights to shareholders to make decisions about any possible transaction related to the funds they invested. The level of control by funders increases drastically this way, empowering them to make any financial decision regarding the investment of the funds inside the company. Furthermore, the new system allows for the creation of a secondary market for tokens; this increases the independence of investors and the security of the market, limiting financial risks and pulling in more possible participants.

During the fundraising campaign, communication between the two parties can still be managed by traditional means of communication offered by the platform; once the campaign is over, communication can be translated in the form of voting rights. Voting systems can be implemented and constructed in different ways, allowing for the distribution of motivations and the reasoning behind certain voting decisions; together with pre-set messages to be distributed to certain individuals according to pre-defined rules of communication.

IT Operations:

The implementation of the technology in the platform, changes the type of interaction that exists between the two parties involved in the transactions. The relationship is handled by smart contracts; IT Operations and coding are therefore fundamental for the well-being of such relationships. The use of the technology allows for an extreme level of freedom in the definition of the relationships. The market is still waiting for the right legislation to define the limitations of this market, but until then, projects and interactions of such sort are highly independent from any regulation and legislation.

Payment:

As we can imagine, one of the most important innovation brought by the blockchain technology is the use of a secure, transparent, and valid form of online payments and registration of transactions among users. This is why the technology has a particularly strong effect on this service. The use of cryptocurrency as one of the possible ways of exchanging value, gives the possibility to different services to come into play in these networks. With the use of cryptocurrency in fact, we can have different integrated or satellite DApps that are able to offer different services to users such as digital wallets or exchange platforms.

These services related to the use of cryptocurrencies have many benefits and drawbacks that we will not analyse in this thesis.

Banking:

Banks could be easily eliminated from the framework, since the central role usually played by these intermediaries is eliminated in a distributed decentralized system, and substituted by the technology. Smart contracts in fact, take care of all financial transactions and contractual relationships between partners; while the history of transactions is recorded entirely inside the blockchain.

Dunning & Debt Collection:

As many other services that could be performed by third trusted parties, smart contracts could be in charge of carrying out these services in a standardized and trusted way. The power of reinforcing these actions could be given to the final users or to enforcers that could work with the power given by voting rights.

One of the possible application of smart contracts is furthermore the possibility to create special funds financed by transaction fees, that could be used as collateral for the eventuality of the need of an insurance repayment. The possibilities are many, and can be similar to the ones already existing in the traditional network; the difference lies in the use of smart contracts, whose execution is mandatory whenever certain conditions are met.

3.3.2. Platform Interactions and Service Provision

In section 2.3.3., we described the structure of interaction between the actors in the traditional crowdfunding network. In this section we provide a description of the same

environment, in which blockchain technology has been introduced.

Figure (16), shows how the ecosystem of relationships and services changes as we introduce blockchain technology. The figure shows the role and the position in the market of a blockchain-based Crowdfunding DApp; a new important element, which drastically changes the structure of the system. This interaction network is in contrast with the traditional system of interaction shown in Chapter II; the number of actor present has in fact changed, together with the distribution of key activities. Some service providers can be eliminated, and their functions absorbed by others. New service providers are able to perform in such a way that benefits the two major actors involved, while introducing a high level of decentralization and reduction of risk, usually associated with blockchain technology.

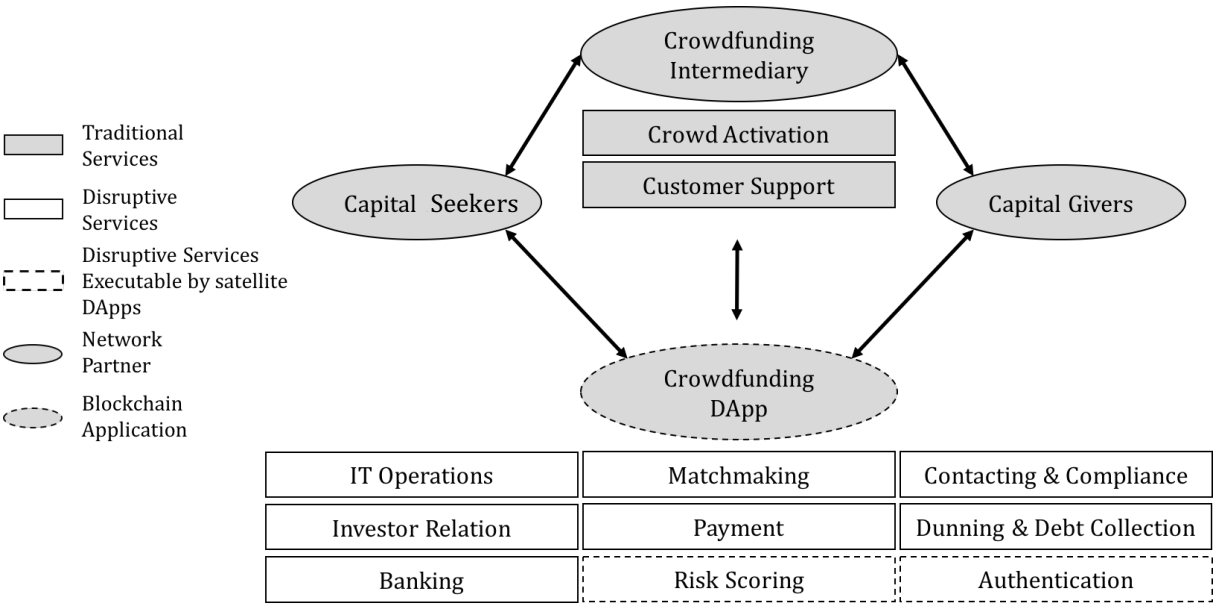


Figure (16): Equity Crowdfunding platform interaction and service provision in a blockchain-based ecosystem through the use of a DApp.

The Figure shows how some of the activities like Banking and Payments, that are traditionally performed by third party members, are embodied inside the DApp. The figure also shows how some of the services like Crowd Activation and Customer Support, are better performed by the Crowdfunding Intermediary such as a traditional crowdfunding platform, rather than a Crowdfunding Decentralized Application.

There is a distinction between the types of services that could or should be performed by a computer programme such as a smart contract, and those that are better performed by

a traditional platform. Not all services can benefit from a total codification and computerization; there are activities that require a certain level of flexibility and adaptation, that computer science is not able to provide.
It is important to notice though, how the DApp is able to integrate in its code, many of the services and the roles that are traditionally carried out by external third parties. These third party service providers like crowdfunding partners and payment providers like banks, can be eliminated from the network, decentralizing drastically trough the blockchain technology many of the most important activities.

3.4. Effects of Decentralized Applications on Crowdfunding Inefficiencies

Blockchain technology can be applied in many industries that are currently in need of a decentralized application. We decided to focus on the crowdfunding industry, because of the extreme growth is has been having in the past few years, and the huge potential that the introduction of the technology has in the democratization of this system.
The crowdfunding ecosystem is in need for a new system of interactions between the parties involved, that will reduce the current inefficiencies and costs, related to crowdfunding. Now that we have explained how the traditional crowdfunding system works and how a blockchain-based crowdfunding system could work; we can explain how the introduction of the blockchain technology could alleviate the inefficiencies currently present in traditional equity crowdfunding platforms.

This section describes how the blockchain technology and the use of DApps and DAOs, can reduce or even eliminate some of these inefficiencies. In order to do so, we will analyse the application of these tools in the ecosystem in three different matters. First of all, we will show the general implication of the application of blockchain technology in the crowdfunding ecosystem; together with the consequences it has in general with respect to market inefficiencies currently present in the market. We will than explain how the functionalities we described of the decentralized application could solve the inefficiencies we identified in Chapter II for the traditional equity crowdfunding ecosystem. We will finally associate some of the features of the equity crowdfunding DApp with the resolution of key financial risks, that through the technology will be reduced and in some cases completely eliminated.

3.4.1. Market Inefficiency Reduction with Blockchain Technology

As we have seen in the previous chapters, the traditional crowdfunding platforms present some major market inefficiencies[29]. These inefficiencies can be summarized by two major problems that represent the market's and network's limitation. These problems are Asymmetric Information and Molar Hazard.

Asymmetric information represents a group of issues that revel themselves before any interaction takes place. Asymmetric information in fact, refers to the different level of knowledge that characterizes the two parties involved before any interaction takes place. While on the other hand, Moral Hazard refers to all the issues that arise once the transaction has taken place and there is a mismatch between what was expected and what actually happens later on trough the evolution of the project.

We will show how with the introduction of blockchain technology, these issues are strongly reduced and in most cases eliminated.

When we introduce blockchain technology and its applications inside the crowdfunding system, we can see changes in the network from the first steps of the crowdfunding process.

Starting from the screening of the possible projects to be presented to the public in fact, the intermediary role of the crowdfunding platform can potentially be eliminated since everyone using the DApp in a decentralized environment, can present their project to the funding public. It is important to note that, on the other hand, this might create the issue of an overflow of information, that will necessitate a system for the assessment of the credibility and reliability of the creators of such campaigns. Mechanism based on reputation can also be implemented in order to allow fundraisers to certify their professionalism and convince capital givers to invest in their projects. If that would be the case, the DApp can, also in this case, come into play by creating a standardized and mechanistic system of reputation and place itself as the trusted intermediary. The importance and the reliability of the reputation system can be seen in notorious examples such as Amazon or e-Bay that base their network on this feature. The success of these platforms, helps us realize how this functionality of smart reputation could really work also in the crowdfunding and sharing economy future ecosystem.

The decentralization of the effort in offering a reputation system will definitely reduce the

[29] Section: 2.5. Ineficiencies

costs of administration and will be more transparent than the current one. The crowd-powered system will than give benefits to both the actors in the market, reducing cost on one side, and increasing transparency on the other.

For what concerns the issues that arise only after the initial interaction between the two parties, they can be lowered through the establishment of forms of security in the DApp that protect the interests of the funders. Hidden Actions can hurt funders, that in a traditional crowdfunding ecosystem have very limited rights and right enforcement mechanisms at their disposal. Once the investment has been processed and transferred to the fundraisers the power of the funders is drastically reduces and they have very little control over the capital invested. The implementation of defined rules inside the DApp to protect the interest of the funders, do reduce the amount of effort required by them to enforce their rights. These rules manifest in the form of Voting Rights and Withdraw Tracking; these rules substantially improve the power that the funders have over the funds they decide to invest in new ventures.
The level of transparency and the implementation of voting right have also the effect of reducing not only the two major problems of Hidden Information and Actions, but also reduce the related problem of the Principal-Agent Problem, giving back the control to those that are directly involved in the funding process. The Principal-Agent Problem issue can be solved also by making sure that both the funder and the fundraiser are in possession of shares or tokens of the company, aligning the interests of the two.
The presence of voting rights and the creation of certain rights on the spending of the funds collected, is of extreme importance for the participation of the funders in the process of crowdfunding. The absence of these rights would not push investors to participate, making the market fail. It is important to remember though, that it is still important that the fundraisers remain an important presence both financially and managerially inside the organization. The designers of the company are probably in fact, the most valuable component when it comes to decision making. They, are the individuals that have the most insight on the industry in which the company will be immersed into, and are probably the ones that will be able more than others, to give the most added value to the company once it will be deployed in the market.

Another major innovation brought by blockchain technology are smart tokens. The introduction of smart tokens has major benefits, in the sense that will allow for the

creation of a secondary market that will not only push funders to invest in more than one company, but will allow fundraisers to collect funds more easily and faster.
The use of smart tokens and the implementation of voting rights on the other hand, might have some drawbacks on the industry. These new rights might allow funders to impose entrepreneurs to pursue more short-term returns rather than long-term once. The creation of a secondary market for tokens might in fact motivate funders to pursue such a strategy, backed up by the improvement of the power they will be able to impose to entrepreneurs. One possible solution to this problem would be a diversification between those that have short term and those that have long term visions or expectations on the projects they invest in. The subdivision of investors on the base of objectives, will allow fundraisers to select their fundraisers, and have a group of shareholders that will not just look at their own interests, but will have interests in the well-being of the company and the project they are backing up. The best decision entrepreneurs can make, is to be part of the investment pool, in order to mix their vision and interests with the ones of the rest of the investors.

The major improvement given by the technology is the fact that it will create a more transparent, decentralized, and democratic way to fund small and big businesses, where the interests of both the funder and the fundraisers are taken into account. Frauds will not be necessarily eliminated, but the fact is that they will be traced and will be permanently written inside the distributed ledger could discourage - more than the system is doing now - malicious acts form happening.

3.4.2. Market Inefficiencies That Could Be Softened by DApp Functionalities

In section 3.1.1 we took a look at the new functionalities that an Equity Crowdfunding Decentralized Application could bring to the table. In this section we will see how these new functionalities can help to reduce and in some cases even eliminate, many of the limitations that the traditional crowdfunding system presents in microeconomic terms.

Crowdfunding Campaign:

One of the first problems related to crowdfunding is the allocation of funds during the crowdfunding campaign. In the traditional system, the crowdfunding platform would have to relate on a third party like a bank to hold the funds, or do it itself. This methodology might raise security and trust issues, which blockchain technology might

resolve.

A DApp application in the first steps of the fundraising campaign, is able to function as a holder of the funds raised. This important function, eliminates the need of the introduction of an external and centralized third party. The funds that are raised during the campaign in fact, are not directly transferred to the fundraisers, but are kept in a separate and autonomous account created by the DApp. Inside these accounts, the funds are locked until the right amount is reached or the campaign expires. These security measures, defined by conditions under which the DApp has to undergo, give the funders a high level of protection on the funds they decide to invest, which improves also their willingness to invest in new projects. These security measures usually consist in thresholds of funds to be reached, or time limits after which the campaign expires. If these conditions at the end of the campaign are not met, the funds invested are automatically transferred back to the funders by the smart contracts embodied in the DApp.

These security measures though, are not constructed to protect just one side of the transaction. Fundraisers in fact are protected too by functionalities of the DApp right after the end of the crowdfunding campaign. As soon as the campaign is over and all the conditions for the project to go on are met, the funds are available to the funders for use through the development of the project, and will be used by them to construct their company. The most important thing to keep in mind is the fact that the amount of rights and protection of the two parties and the resolution of the market inefficiencies, can be pre-determined through the coding of the smart contracts. The goal would be though to create a balance between the two forces and allow both parties to work in an environment that is transparent, and more importantly, secure.

Smart Property Tokens:

As we previously pointed out in section 2.5.1, traditional equity crowdfunding platforms do not allow for the creation of a secondary market for the exchange of shares. the Smart Property tokens in a blockchain-based crowdfunding platform, will substitute the role of shares and will than revolutionize the financial market. Blockchain technology makes it not feasible to falsify tokens and ownership of certain assets, allowing for a riskless and costless marketization of them.

The introduction of a secondary market for tokens, revolutionize the equity crowdfunding market; in the sense that gives investors the possibility to exchange tokens freely and in a secure way. This is not the only upside of the creation of a secondary market; in fact, this

option gives them the chance to avoid many complications related to the investment in new companies, like the Principal-Agent Problem we discussed earlier.

Decentralized Autonomous Organization (DAO):

The utilization of the DAO structure, allows for the adaptation of the system is such ways that allows for the customization of the project involved, in line with its needs. Most important feature of the technology that interacts with the DAO is the voting system, that increase exponentially the resilience of the project. This feature supports any decision that can be made by the participants. These decisions can include also the relocation of the project into a new blockchain service, that might fit better the company needs.

All of this allows for the empowerment of the investors; that will have more control over the funds they invest, and more control over the actions of the fundraisers.

Funders have an exceptionally high control over the funds, making them in charge of almost any decision that the company is deciding to undertake. Funders have in fact, control over all the accesses to the company funds, making them able to allow or not the use of the capital by managers and owners. By having control over the funds; there is a consequential strong reduction of the principal-agent problem.

Voting System:

When we are dealing with equity crowdfunding, the risk of fraud by the fundraisers to the detriment of funders is significant. Having a substantial amount of control over the funds invested than, has particular importance in these situations. The voting system is designed and has been created specifically for this purpose. With the voting system, the risks are reduced by creating this right enforcement mechanism that gives the power to funders to control the funds they decided to invest in the venture.

The DAO is able to create a democratic environment, allowing shareholders to be part of the decision making process and enforce actions.

This security mechanism works as a deterrent for managers to undertake selfish or malicious acts that will hurt the company, and consequently share or token holders. This can be considered an initial solution, to the principal-agent problem and the moral hazard problem.

The increase of control by users, is not the only benefit brought by the application of these mechanisms. More automated control means that the costs from actual control performed by the funders, are substantially reduced.

Probably the most interesting consequence of the introduction of the voting mechanism, is the possibility to leverage on the so called "Wisdom of the Crowd". Voting mechanisms can be implemented at multiple levels inside the DApp, this means that funders can decide where their knowledge could be of best use inside the organization. Every step and function carried out and necessary inside the organization, could benefit from hidden knowledge inside the crowd that funded the organization. The positive intervention of the crowd is not just limited to the crowdfunding campaign and the money management, but especially extends to situations in which their knowledge could be crucial for shaping the company's strategic path.

The introduction of such voting rights is the clear example of the potential of the decentralization brought by blockchain technology. Voting rights are one of the major features of a democratic system; where the decision making power is not in the hands of few, but in the hands of all the participants to the network.

Withdraw Tracking System:

The withdraw tracking mechanism introduces two important functions, that have as a consequence two important benefits within the crowdfunding system.

The fist function is the ability for the system to create a limit to the amount that the manager or the entrepreneur can withdraw from the funds that have been accumulated. This mechanism creates a balance between the two parties involved, allowing for a decent level of freedom of movement for the managers, and at the same time a fair amount of control of the resources for the funder. This also reduces the principal-agent problem, creating an equilibrium of the forces.

The second function allows for the introduction of a higher level of transparency. The function in question is the unquestionable truthfulness of the transactions that are written on the blockchain. This mechanism makes it very hard for anyone to make malicious or suspicious transaction with the funds stored in the DAO. Moral hazard is therefore reduced drastically, and frauds become traciable.

These rules allow the funders to have two separate control over the money that they invested; they are able to vote for allowing a transaction to go through, and they are able to keep track of all the transactions linked to the funds they helped raise. Transaction that do exceed the conditions previously set between the two parties, are on the other hand automatically blocked by the code.

Control over the money invested is one of the major democratic improvement that the

blockchain technology introduced.

Risk-Scoring System:

Asymmetric information in the crowdfunding market can still be an issue even in a blockchain-based environment. It can be hard in fact, to collect information and verify the credibility of fundraisers. There are though, systems to overcome these issues that can be built in one of the DApps that works in the environment. These systems can come in the form of "Reputation Systems" and "Historic Scanning". Such functions will help funders to have a view of the past experiences of the fundraisers they would like to invest in, and will give them a general view on they reputation they built around themselves through past projects.

These functions can be performed by a secondary or satellite DApp; or even implemented and be automatically activated inside the main crowdfunding DApp. These functions can also be performed by an external third party like an external financial institution that is able to access information about the past financial records of the fundraiser. Confidential information does not have to be divulged necessarily, but the solution might be the creation of a smart contract that allows for the assignation of a score to each individual, defining their reliability based on their credit history or past transactions.

Some crowdfunding platforms may also decide to have their own system for the definition of the risk related to an investment. It is important to keep in mind in fact, that the risk associated with an investment does not only depend of the financial record of the fundraiser, but also on the feasibility of the project presented.

The modalities with which fundraisers can be screened and categorized can come in different forms with different levels of complexity. The concept to keep in mind is that the blockchain technology provides a framework for the registration of all economic activities, transactions and movement of ownership. Traceability of currency, assets and interaction is extremely accurate allowing for a substantial reduction of the problem of Adverse Selection and Information Asymmetry. As the network gets more secure with the resolution of these issues, users will be more willing to participate to the network, making it even more secure.

Smart Identity Authentication:

Particular attention is naturally given to the issue of security in the crowdfunding ecosystem, and on any web platform in general. It is important for any user interacting

with someone else on the platform, to be exactly sure to whom they are talking or interacting to.

When exchanging information or investments, anyone must be able to trust the identity of the person they are interacting with. Smart Identity functionality has been constructed for this purpose specifically.

Through the use of smart identity authentication, the fundraisers are disclosing their identity to the public, showing willingness to be cooperative and transparent. This may induce investors to trust the fundraiser that makes them able to have a full view of their credit history.

Funders can also use smart identity authentication, allowing other users to learn from their experience as successful funders, and push them to participate themselves to lucrative campaigns or investments.

Smart identity implementation can also have positive consequences from a legal point of view. Since actions can be linked more easily to people with no margin for errors, responsibilities can be associated to the right identity easily and fast. The process of identifying people will then be simplified, and costs will be reduced together with the risk of moral hazard.

The use of a digital and secure identity, will not only help governments and debt collection agencies perform a more accurate job, but will also allow users to be entitled completely to their identity. They will be able to control and share at their will their personal and sensible information, without going through a third party whose integrity could not be proven for sure.

Table (3) represents a summary of the possible applications and functionalities of the crowdfunding DApp we discussed, associated with the possible inefficiencies they have been created to soften.

Functionalities	Application Possibilities	Softened Inefficiencies
Crowdfunding Campaign	Self-governing Management of Funds	Moral Hazard & Adverse Selection
Smart Property Tokens	Investment Trading	Principal-Agent Problem
DAO	Self-governing Management of Funds	Moral Hazard & Principal-Agent Problem
Voting System (DAO)	Rights Enforcement	Moral Hazard & Principal-Agent Problem
Withdraw Tracking (DAO)	Transparency	Moral Hazard & Principal-Agent Problem
Risk-Scoring System	Screening	Adverse Selection
Smart Identity Authentication	Right Enforcement & Screening	Moral Hazard & Adverse Selection

Table (3): Inefficiencies softened by functionalities od a decentralized crowdfunding application.

What we analysed in this section can be considered some of the major positive influences that an Equity Crowdfunding Decentralized Application can bring to the crowdfunding environment. Many market inefficiencies of the traditional equity crowdfunding environment can be mitigated thanks to the technology. The improvements will create a more decentralized and transparent environment, in which both actors will be more willing to participate and enlarge the network.

3.4.3. Financial Risks That Could Be Softened by DApp Functionalities

In section 2.5.2, we took a look at the possible risks associated with the use of an equity crowdfunding platform. In this section we will see how the introduction of a Crowdfunding Decentralized Application and blockchain technology, could reduce risks usually associated with traditional crowdfunding platforms.

Through this section, it is important to keep in mind how with the use of blockchain technology, the need of a trusted third party is strongly reduced. The trust shifted from centralized parties, to the decentralized network and the technology.

Risk of Default:

Risk of default, in a crowdfunding decentralized application, can be consistently reduced thanks to the first phase of the blockchain-based crowdfunding process. During the

funding stage, the funds are not directly transferred to the fundraiser, instead they are put in a separate account. The account will be unlocked and the amount transferred to the DAO in the case in which the campaign is successful, or given back to the funders in the case of failure of the campaign.
During the period of time in which the funds are managed by the DAO, the mechanism associated with it, makes sure that the funds are secure, and transactions not allowed. The control in this case is of the funders, that will act in their interests and the interest of the company they invested in, mitigating the risk of default. The funders can in fact impose control over the funds through mechanisms like the transaction spending limit and the voting system.
These are the early stages of the application of the technology, in the near future, new developments could lead to the creation of algorithms that will improve furthermore the avoidance of this risk, like stronger reputation system mechanisms or better mechanisms for the selection of fundraisers.

Risk of Platform Closure:
One of the characteristics that distinguishes blockchain technology is the fact that it is not centralized; the decentralization of a DApp in fact, allows it to be impossible to be shut down, since it is dependent by the network. In a decentralized system, the DApp is the one that holds the most important function for the crowdfunding network to be carried on, while the crowdfunding platform covers services that can be substituted by a secondary entity right away.
Whenever a platform is shut down, the related DApp and the smart property that used the platform to enter the network do not disappear, since they are dependent from the network that will not be effected and continue to run.

Risk of Fraud:
The use of a blockchain-based application has the potential to reduce drastically this type of risk, through the use of many of the functionalities that we have seen so far. To name a few: Voting Rights, Transaction Spending Limits, Unforgeable Smart Tokens, and so forth. Together they are able to offer users a transparent environment, in which actions of fundraisers are permanently recorded into the ledger, making it nearly impossible for them to let their actions go unnoticed.
Moral Hazard and Risk of Fraud are closely related, meaning that further development in

functionalities such as the attribution of Credit Scores, will influence also the reduction of this financial risk.

When using this new technology, we need to pay particular attention to how these new mechanisms could be perceived and understood by the public. The structure of the coding, and the meaning of some smart contracts could be tricky for many of the users approaching the network for the first time. One possible solution is to rely on well-known platforms, credible establishments, composed by individuals that have the reputation of creating fair and standardized smart contracts and DApps structures, approved by the public or experts in the field.

Liquidity Risk:

As we have seen in Chapter II, the technology introduced the concept of smart property, and with it, the possibility to trade smart tokens freely on secondary markets. Smart tokens can be than traded, transferred, and sold freely without having to hold them until maturity. We underline the importance of this feature, that allows investors to commit to shorter investments horizons; a characteristic of major importance when it comes to start-ups and the crowdfunding environment.

The characteristics associated with the technology and more specifically smart property, are than allowing for a substantial reduction in the risk of liquidity inside a blockchain-base environment. The technology and this framework are able to create different, easier, and more unaffiliated equity crowdfunding platforms.

Risk of Cyber-Attack:

Since the whole system relies on the internet in order to function, the issue of cyber security arises. The nature of the blockchain technology though, makes it extremely hard for a decentralized ledger to be hacked. In order to hack an entity constituted on a blockchain ledger, and manipulate information that are stored inside it, the hacker would have to be able to have simultaneous access to the majority of the nodes that compose the network. Such an attack, called the 51% attack, would require an unthinkable amount of computing power, and un unthinkable amount of Gas to complete that operation.

One of the other few precautions to take is the way in which smart contracts are constructed. Smart contracts are not flawless if the coding is not done right. There are companies that specialized solely on the development of such contracts, which are a good starting base for whoever is willing to create their own DApp.

Potential Systemic Risk:

Systemic risk is linked to the liquidity risk. In a traditionally constructed market, the exchange of stocks or tokens can happen also between parties that work in different countries or under different legislations. The process of interconnection between different legislations and possible different currencies, usually slows down the selling process and can lead to liquidity risk.

At the time of writing, the legislation about cryptocurrency and blockchain-based crowdfunding is not well defined, meaning that blockchain-based infrastructures are for now still independent form any form of national or international legislation. The decentralized nature, and the use of digital protocols for the management of activities and transactions, allows many to ignore any national legislation in term of movement of currency and value. The lack of a proper legislation on the other hand, is discouraging many in the pursuing of blockchain-base crowdfunding projects, for the fear of developing a project that might be shut down as soon as another legislation becomes valid.

Many countries are developing at the moment their own legislation on the crypto market and in the first few years of the development of the technology we might see a separation between some of the major market like the American one and the European one. Once the technology will have settled and will be understood by all legislators, the internet nature of the technology and the process, will allow for a merger of all the major market and the creation of a global and open one.

CHAPTER IV

Blockchain-Based Equity Crowdfunding Platform: The Bloomio Case

While looking for a case study, we realized how difficult is to define legally an entity that works on the blockchain; and especially how hard it is to define the legal and financial identity of a token.
We live in a technological era in which we have very few insights on what, when, and how complex and disruptive innovation will appear in the market, putting regulators in a thought decisional position. Regulators are battled between the creation of a fast and responsive regulation, usually not backed up by sufficient information; or legislative paralysis, resulting in a procrastination of the tackling of the issue. The commonly used strategy is the one that uses caution, that has the result of stabilizing already established technologies, limiting an efficient and punctual introduction of new innovation in the market.

It is important to inform the reader, that given the early stage of the life of blockchain technology, each country is currently developing their own interpretation of the identity of tokens and blockchain-based applications. For now, in fact, no legislation or regulation has been formed, that refer to the legal parameters around blockchain technology or tokens. The difficulties in the definition of a common ground in the crypto market, is unfortunately resulting in a sub division of the global market.

In this chapter we will analyse one of the first examples of a blockchain-based equity crowdfunding platform that we had the privilege to come in contact with. The platform is called: “Bloomio” and is based in Switzerland, in what is becoming to be known as the “Crypto Valley”, in the canton of Zug.
The platform is still under construction and the team is working on the development of all the most important services and functionalities, while collaborating with the local government for the definition of the legal status of the company and most importantly of the tokens that it will issue. The purpose of this chapter is to explain how the concepts that we analysed in theory, can be actually implemented, and what can be the adaptations necessary for a real physical application.

4.1 The "Crypto Valley" Regulation

Since Bloomio has its legal headquarters in the so called crypto valley, it is important to understand how this region gained this epithet, and what are the advantages of starting a blockchain-based business in the canton of Zug.

The crypto valley is positioned in a region that is mostly known for its decentralized political system, and matchless business environment. The region of Zug offers high possibility of growth with its pro-business environment, acceptance, and accessibility of the local government. The region attracts many international and leading companies with a system that allows for a low taxation, culture of financial privacy, and a business-friendly environment. The region is in fact the crypto-powerhouse for companies like Ethereum, Xapo[30] (Bitcoin wallet), Shapeshift[31] (global web trading), Monetas[32] (financial services for unbanked individuals), and Melonport[33] (digital investment fund), together with many others.

Even though a proper legal framework has not been developed by any country yet, the regulatory framework of the canton of Zug seems to be a lot less restrictive and more open to discussion, than the rest of the European governments.

Switzerland is also ranking as the first country in the world for attracting and retaining talent as well as competitiveness and productivity. Furthermore, the political system in Switzerland is neutral, stable, highly responsive, citizen-controlled, and decentralized; all these characteristics are in line with the bottom-up approach of the blockchain technology and the crypto technologies that are emerging.

4.1.1. Crypto Valley Association

All the favourable characteristics of the Zug environment, and the increasing interest of entrepreneurs in blockchain technology, has led to the formation of what is known as the "Crypto Valley Association" (CVA). This association is independent, government-supported, and has the aim of creating the world's leading blockchain and cryptographic technologies ecosystem, taking advantage of the region's advantages. The association wants to create a network to support and connect start-ups and fully operational

[30] https://xapo.com/
[31] https://shapeshift.io/#/coins
[32] https://monetas.net/
[33] https://melonport.com/

enterprises, bringing them together in the effort to foster blockchain and cryptographic technology.
One of the most important aspect of the existence of this association, is the fact that it is collaborating with the government in the definition of a favourable legislation that would foster the development of blockchain-based business in the region.
On December 11th 2017, President of the CVA Oliver Bussmann, was invited to represent the association and the crypto technology industry, at the Swiss Government's second Fintech Roundtable; in which the future structure of the legislation on cryptography and blockchain technology was discussed. According to Bussmann, the government will develop a principle-based approach for the management of ICOs, allowing for a certain level of freedom of movement, rather than a precise definition of inviolable rules. Guidance will be nonetheless allowed to be provided by self-regulating associations (like the CVA) and the government itself in the case of the need for clarification.

The great advantage of the Swiss legislation is the fact that technically, any citizen is able to recommend a change to the law though what is called the Swiss "Direct Democracy". This gave a great momentum to the introduction of the blockchain technology and its potential. The first steps in the creation of a valid legislation, were done in June 2016, when three blockchain-related proposals were presented to the Swiss Parliament's Federal Assembly. These motions had the aim of simplifying the process of anticipation of the ramification of the blockchain technology by the financial sector[34], improve the leading position of Switzerland in the field of blockchain technology[35], and facilitate the growth and the development of blockchain-based start-ups[36].
Unfortunately, those motions were denied, but it did not stop Switzerland progressive way in defining a strong and protected market for crypto technologies.

Crypto Valley Association's Code of Conduct
The most recent achievement in the field of crypto technology regulation, comes on the 9th of January 2018 from the crypto valley association, that in accordance with government regulators, was able to construct Switzerland's First ICO's "Code of Conduct" (CoC).

[34] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163380
[35] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163484
[36] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163472

The code of conduct has the aim of bringing clarity to the new market, and guide properly ICOs on how to conduct in accordance with legal, moral, and security obligations.
The authority carried out by the CVA, makes the CoC mandatory to follow for each company that wants to participate to the market and be part of the CVA.
The declaration is updated annually, and is composed by values and principles agreed upon and respected by all members.
The Code of Conduct is divided in four main chapters: Mission, Core Values, General Code of Conduct (CoC), and Decentralized Ecosystem (DE) Code of Conduct (DECoC).
Their mission is to:

"Develop the World's Best Ecosystem for Blockchain and other Distributed Ledger Technologies and Businesses.[37]"

Around this concept, and around the principles of decentralization and of democratization that the blockchain technology is linked to, the core values have been agreed to be: Trust, Transparency, Collaboration, Integrity, Innovation & Quality, and Security Beneficence. These values are strongly in line with the principles that are behind the creation of the technology. On the plus side, these concepts and rules will be reviewed annually, in order to keep up with technological and organizational changes.
The core of the code of conduct includes guidelines on the Business Conduct as well as guiding on the "Governance" and "Conflict of Interests", "Property Rights" and also important guidance on the procedures for "Disciplinary Actions".
It is important to note also, that the CoC gives guidance also on the "Books and Records" procedures. For this purpose, the CVA has established a partnership with PwC[38], together with which they launched on January 18th 2018, the first of what is being established as the "Quarterly Report on Initial Coin Offerings[39]". The main purpose of this standardized report is to track the evolution and the development of the industry, which is still going under a quick expansion and through continuous changes.
The Decentralized Ecosystem Code of Conduct has been created in order to ensure that, the launch of any activity inside the Association, is done in compliance with high

[37] https://cryptovalley.swiss/codeofconduct/
[38] https://www.pwc.com/
[39] https://cryptovalley.swiss/crypto-valley-association-collaborates-with-pwc-strategy-on-ico-report/

standards of protocols, quality and ledger enforceability, as well as in line with regulations on financial markets.

4.1.2. FINMA interpretation and Legislation on Tokens

FINMA is the Swiss Financial Market Supervisory Authority, and starting from September 29th 2017 - due to a substantial increase in the ICO conducted in and from Switzerland - it decided to investigate the ICO phenomenon. FINMA recognizes the potential of the technology; however, since each ICO differentiate from a technical, functional and business stand point, an analysis of the phenomenon was mandatory to determine the legitimacy of this new funding methodology.

At the moment, as the investigation goes on, FINMA warns consumers on the risks associated with ICOs. ICOs are subject to high price volatility, and usually backed up by early stage and consequently highly risky projects, with very little or no guarantee for future development. The general warning was addressed to the general public, driving the attention to the recognition of fake cryptocurrencies and fraudulent activities, given the recent market circumstances. The government and FINMA transparently admit they do not have all the answers in the field of crypto technology; they are moving forward as fast as they can and together with the public, constructing a system that would not limit innovation and would foster economic growth.

Regulations specifically related to ICOs, are not present in Switzerland or in the international legislation system. What is present on the other hand, are regulations and laws on Equity and Debt capital-raising, deposit-taking and all activities managed by financial intermediaries. These laws have been created to protect both sides of the markets together with the intermediaries involved, in order to have a functional and optimal financial market. This means that in some situations, some ICOs might already be covered by existing regulations, and whenever an ICO issuing tokens, breaks regulatory law or is designed to circumvent financial markets law, enforcement procedures are initiated.

This regulatory system allows than for the creation of ICOs and tokenization of equity, given that issuers and other participants will analyse their projects, determining in which existing Swiss regulation the structure of the project and the functionalities associated to the tokens fall.

A broad approach will be taken by FINMA in the assessing of ICOs and TGEs (Token Generating Events), from which an analysis will originate of the functions and attributes of ICOs, as well as an analysis of the purpose, functionalities, and legal state of tokens. Tokens in particular, have an extremely important role in this industry, both in the Swiss economy and in the International economy.
There are existing regulatory areas in which a TGE or ICO could currently fall in the Swiss regulatory framework, and they are listed below as:

- Provision for coping with money laundering and terrorist funding: Whenever the production of a token by a TGE involves activities of financial intermediaries (money transfers), the provisions refer to the Anti-Money Laundering Act.
- Provision on banking law: The application of the banking regulation is set off whenever there is the acceptance of public deposits as an obligation of repayment to token holders.
- Provisions on trading of securities: If the situation occurs in which tokens qualify as securities, the token issuer is required to have a security licence.
- Provisions in collective investment schemes legislations: Whenever assets aggregated as components of the TGE are managed by an external party, a potential link to collective investment schemes legislations could appear.

MME[40] is a Swiss legal, tax, and compliance consulting firm, that has been working with many companies (including Bloomio) inside and outside the blockchain environment, in order to help them to be in complete legal compliance with Swiss and international regulations on business law.

On September 26th 2017, MME has published an individual and self-regulated framework for the definition of tokens called:" Conceptual Framework for Legal & Risk Assessment of Blockchain Crypto Property (BCP)" (Dr. Muller L., D. Meyer S., Gschwend C., Henshel P., 2017). Luka Muller, one of the funders of MME and CVA, specifies than the definition of token that has been provided in the paper, is not the definitive definition, but on the contrary the "Genesis Version" as they called it.

[40] https://www.mme.ch/

The main aim of the paper it to educate the public on this new technology by creating an initial framework to define the elements that compose it. Highly important for users though, is also the definition of the risks associated with this new technology, able to improve their investment plans, but to which they need to pay extreme attention.
The paper introduces the definition of tokens as a new type of property, or better, Blockchain Crypto Property (BCP), which are divided in three main categories. The division of the BCP in categories has been done to facilitate the construction of an easier legal, regulatory and tax assessment for different types of tokens, as well as an easier risk assessment.
The three major token categories are called respectively: BCP Class 1 (no counterparty), BCP Class 2 (counterparty), and BCP Class 3 (co-ownership). We provide below a brief description of the three classes of tokens.

BCP Class 1:
Are native currency tokens, infrastructure tokens or application tokens; which do not give the owner any right with regard to a legal person, and cannot be associated with a physical asset.

BCP Class 2:
Grant right against a legal counterparty. Contractual and participation rights, can be considered as Class 2.

BCP Class 3:
Are tokens which have specific functions programmed inside them, are registered and store on the blockchain, and use the technology associated with smart contracts. Co-owning right are reinforced by the use of these tokens, and the holder of the tokens can participate in the co-ownership of physical or intellectual property.

Risk associated with the technology and the use of tokens have been divided in four major risk classes: Functionality & Protocol-Related risk, Storage & Access of Private Key-Related Risk, Regulation & Money Laundering-Relate Risk, and Market-Related & Counterparty Risk.

The use of a functionality-based method for the classification of tokens and the relative risks, rather than the use of a specific country's legal concepts, allows for an application of these definition to all jurisdictions, disregarding the national or international regulatory frameworks. Related to the definitions provided in the MME paper, different national legislations may arise; but at least the public would be informed on the technology and the tokenized ecosystem, having a common knowledge of the characteristics that define a digital property and coins.

MME also gives a list of advices to anyone willing to start a blockchain-based or token-based project. The first one is to be smart; it is important to figure out the companies blockchain and token functionalities. All the information and the definition of the business case and legal analysis must be defined, in order for the project to unfold positively.
The second recommendation is not to commit fraud. As simple as it may sound, the importance of a good disclosure commitment about the project and the related tokens is important in this new market and for the community.
Thirdly, MME advises new entrepreneurs to think globally, meaning that the compliance on regulations should not be done just on Swiss law, but also on international law.
Taxes should also be considered whenever carrying out these projects; the understanding of the related tax system is of extreme importance during a token launch.
Finally, communication is of extreme importance during and after the token launch. The fundraiser owes to the investing public, to let them understand what is happening to their investments.
MME is a strong partner of Bloomio, and it is helping the company to be in complete compliance with regulations in order to enter the market in complete safety and compliance.

4.2. The Origin of Bloomio, The Vision of the Funders and the Legal Battle

The case study we analysed in this thesis is the one of Bloomio, an equity blockchain-based crowdfunding platform, that will presumably change the conventional way of doing business for companies in the field.
We had the chance to interview Maxim Lyadvinsky, Bloomio's Chief Executive Officer (CEO); and Francesco De Santis, Bloomio's Chief Marketing Officer (CMO). Thanks to their

testimony, we were able to understand what their company stands for and why this platform came into existence.

The idea of the company started from the definition of the problems related to Venture Capital funding; with all the issues that go from liquidity, lack of capital, risk of fraud and limited quality information.
Bloomio has been funded by three associates coming from different fields, in which each one of them have been successful. The three funders are Maxim Lyadvinsky, former founder of Acronis, that has been working, investing and developing multiple start-ups; Emile Osuba, a successful finance executive that can count on 17 years of experience in a top European financial bank; and Alexey Raevsky, cybersecurity and blockchain expert.
On November 2017, Luka Muller, one of the main figures of MME, joined the company as the legal, tax and compliance advisor; in order to help the company to be in complete compliance with Swiss and International law. This figure will be of extreme importance inside the company in order to maintain the highest legal integrity, and to cross - with the highest level of expertise available - the "legal grey area" around blockchain.
Bloomio defines itself as the first platform that will initiate the journey of perpetual reform in the process of funding start-ups, by also enabling investors to invest in new ventures with as little as fifty dollars.
Bloomio funders recognized the growth in the industry of capitalization of start-ups and the increasing importance and potential of blockchain. The funders also recognized the limitation of the current state of ICOs development and evaluation, and realized that a crowdfunding platform that would resolve many of these issue, have not been created yet.

Bloomio also participated and was recognized as one of the 25 winning start-ups in the competition held by the "International Institute for Management Development (IMD)", former school of the funders, where they first decided to create this platform. This positioning in the ranking increases their notoriety inside the start-up ecosystem, and together with that, allows them to work directly with some of the best MBA Students at IMD during the first half of 2018 as well.

4.3. Competitive Advantage and Key Features

Bloomio partners and collaborators, have years of experience in many fields, starting from management, blockchain technology, cyber security, finance, law; and can count on being settled in one of the most technologically and regulatory developed regions of the world.

What Bloomio offers is the highest financial standards to start-up investments for both sides of the market. Bloomio has a set of services designed for investors and fundraisers, that would help both achieve their goals and create a more transparent, free and secure market.

4.3.1. Competitive Advantages

Financial integrity is one of the major concerns for the Bloomio platform and its partners, that decided to construct the platform around this concept, creating a fair, transparent and valuable crowdfunding platform for projects and for investors willing to invest in them. Starting from this concept Bloomio has five major advantages that is proposing to the market of equity crowdfunding.

Blockchain Technology:

Blockchain technology allow for financial transactions to become highly secure, and protects investors and fundraisers. Furthermore, the promise of decentralization brought by blockchain technology, will change the rules of the game. Even if it is still an emerging technology and we are just starting now to see the full potential, Bloomio really believes blockchain technology to be the next frontier in the creation of a better business environment.

"Blockchain is necessary as a mean to transmit to our customers what the main values of the company are; and explain the financial and transparency standards missing on other platforms"

Francesco De Santis (CMO)

Blockchain will help reach new markets and especially new customers, involving anyone who is willing to invest in valuable projects, regardless of the financial availability. Francesco De Santis said in the interview:

"Our Target will be those willing to spend between 1000 and 20000 SFr, a bigger audience than other venture capitalists, but equally hungry for investments"

Francesco De Santis (CMO)

On the plus side, the application of the technology brings a new and higher level of security, transparency and freedom, that has never been proposed in the equity crowdfunding market. The advantages of the use of blockchain has also a more practical benefit; some characteristics of the technology allow for the reduction of the project related documents, with consequent benefits for the security of information stored on the blockchain, which are untouchable by anyone.

"Regulators are more comfortable in approving our operations if we show that we cannot access user's funds and cannot alter user's transactions stored in the blockchain."

Maxim Lyadvinsky (CEO)

Banking and Security Background:

Bloomio's executive team is compose by valuable and professional individuals, that take the issue of security very seriously. Alex Raevsky is in charge of cyber security inside Bloomio; together with Emile Osuma - in charge of the banking structure - they have developed a solid and safe environment. Security is one of the main concerns for Bloomio, that realizes the limitations and the threats that can come from an on-line service, especially when there are investments involved. Bloomio can count on the many years of experience of its collaborators and the strong trust that exists between them.

For what concerns banks, the relationship of the platform with them will be limited to investment opportunities. The use of the technology will allow for the elimination of the banking intermediary, but the interaction with them could still be of importance for the construction of investment opportunities for banks and their clients in emerging start-ups.

"We'd like to collaborate with banks, offering access to alternative investments from their banking applications"

Maxim Lyadvinsky (CEO)

Blockchain has a major role also here, in the creation of a secure and decentralized environment. The technology offers in fact a very high level of decentralization and security measures, with really low costs of administration for the platform.

Expert Broad Due Diligence:

Whenever a project is presented to the platform - in order to present to investors valuable investment opportunities - a due diligence analysis is necessary. Differently from the other platforms, Bloomio has decided to rely on third party evaluation.

"The use of a third party due diligence practice, avoids the possibility of our platform to make a biased evaluation of the projects. We want to give investors the possibility to invest in valuable, profitable and safe projects not directly promoted by us."

Francesco De Santis (CMO)

Due diligence is a very delicate matter and is one of the most important services that a crowdfunding platform could provide. Bloomio wants to be as unbiased as possible and give the possibility to users to invest in valuable and profitable projects, backed up by a well-defined structure and business plan, profitable and secure for all the parties involved.

Swiss Quality:

Swiss quality plays an important role in the definition of the validity of the Bloomio Platform. The favourable regulation, the business oriented environment and the decentralized government of the country, makes it the perfect environment for the development of projects like Bloomio. Bloomio wants to make sure also to be in complete compliance with Swiss and International regulations, and it is the reason why Bloomio included Luka Muller in the advisory board of the company.

"Government regulators are currently not willing / able to provide any guidance in this field, which is why we need to lay the legal foundation for these types of project. Our team has done quite some work regarding the tokenization of shares (or creating so called crypto shares)"

Maxim Lyadvinsky (CEO)

The connection of the company to one of the major legal experts on blockchain and "crypto technology", shows how strongly the company feels the necessity to be in complete compliance with the law; and how valuable their experience and the Bloomio project can be, in helping the development of new regulations and legislations. The collaboration with self-regulating entities, will not only foster the growth of the industry, but will benefit all the actors involved in this new crypto market.

Process:

When interacting with Bloomio, users can benefit from the multiple tools available for the definition of what are the best projects for them and when ready, invest easily and in a safe environment.

Thorough analysis of the projects presented, selection of partners, investor relations and the multiple services available, is what defines the process presented by Bloomio. According to the company, this process will not just connect private investors with start-ups in need to raise funds, but will create a comprehensive structure that aims at maximizing investment opportunities with a series of unique features.

4.3.2. Bloomio Key Features

In order to distinguish itself from the rest of the equity crowdfunding platform, Bloomio presents some indistinguishable key features that makes it unique in the current state of the European crypto technology market. Some of these features are dependent from the relationship that the platform has with blockchain technology; but others are developed to be an evolution and an improvement of what is currently been offered in the equity crowdfunding industry.

Start-up Ranking:

Before the publication of a new project on the platform, the feasibility of the project needs to be accessed properly. Bloomio puts extreme importance to the application of a proper due diligence, to be able to present to investors valuable and profitable projects, while at the same time pushing fundraisers to develop better projects with higher chances to be funded properly.

Due diligence procedure is left to an external and unbiased third party, which issues a five star ranking system, that helps investors evaluate the potential and the risks associated with the investment in a projects. The five key points on which the evaluators focus on for

the definition of the scores are: The Team, the Product Idea, the Level of Innovation, the Product State, and the Product Maturity; these five evaluation point constitute a fair base of evaluation for each project. Showing the result of the due diligence is mandatory for all the companies that want to raise funds; but most importantly, start-ups with one or two stars are not allowed to raise funds for a period of six months, after which a new due diligence report is filed.

The evaluation of each project is customized around the structure of the project being evaluated, and around the nature of the industry in which that project will be placed. The evaluation of the presented projects is the first step in the creation a valuable, stable and transparent equity crowdfunding platform; we can see from the measures employed, that Bloomio and its collaborators understand very well the importance of these procedures.

Start-up Acceleration:

Bloomio aims at helping start-ups to raise capital, but its effort in the development of valuable entities is not limited to that function. The platform in fact also helps new companies to create a structure of connections that will help them grow in the industry they are entering. Bloomio has created a network of third-party services to be connected with start-ups and help them build their team, R&D processes, go-to-market strategy, salesforce, and everything they need to grow and scale.

Bloomio is able to collaborate and help different levels of start-ups. One of the other characteristics that differentiate Bloomio from the rest of the market, is the fact the platform recognizes that, it is not just the early stage start-ups that need funding. Some start-ups need funds to make their business start, but other already established firms, may need funds to scale operation and exploit the full potential of the idea. For this reason, Bloomio has created four different start-up categories, that would make it easier for users to identify the type of company they are deciding to invest in. The subdivision is composed by: Seed, very early stage companies which are raising funds to establish operations; Series A, in which some preliminary KPIs have been developed and need funds to translate ideas into a reality; Series B, in which there are already revenues, but growth needs to be fostered with funds; and finally Series C, for which the main focus for funds would be to scale business to exploit its full potential.

Tokenization:

Blockchain technology allowed Bloomio to implement the tokenization of start-up equity, in order to simplify transactions, and make investments more secure and transparent. Tokenization facilitates the investment procedure for both funders and fundraisers. Funders have an easier way to support the start-up they believe in, and fundraisers have a faster and a lot more functional way to reach their goals.

Each start-up is in charge of determining how big is the share they are willing to tokenize and what will be the price of each token. Bloomio helps them in these decisions by keeping available all the supportive services necessary.

Bloomio will also provide the service of holder of tokens, acting as the custodian of the start-ups shares. The platform will give the service of issuing the start-up tokens that represent the equity of it, in complete accordance with start-up founder's decisions.

Bloomio is a pioneer in this industry, and together with the government is learning how the industry works and how it will develop in the future. There are many difficulties in the creation of a profitable and regulated entity, given the fact that they cannot rely on others experiences.

"Bloomio is the first project that tries to tokenize individual shareholder's rights (in this case the right to participate in the proceeds of liquidation and sale) and trade them on the blockchain, so there is unfortunately not much prior work we can rely on."

Maxim Lyadvinsky (CEO)

Secondary Market:

As a consequence of the tokenization of equity, the creation of a secondary market for tokens is one of the most important and interesting features that Bloomio has implemented. The possibility to exchange tokens after the end of the campaign is an important tool in the equity crowdfunding ecosystem. Investors are able this way, to manage more efficiently and strategically their investments and protect their interest a lot more easily with respect to the traditional equity crowdfunding methods.

The Bloomio market for tokens is now only restricted to the internal projects and available only to the direct users of the platform. This choice has been done for two major reasons that were brought up by company layers. Mr Lyadvinsky explained how some of the projects that are supported by the platforms, may have some problems in the identification of the customers. As a consequence, the companies might have problems in

the determination of who is the person in possession of tokens. Tokens could go through unknown hands and become "dirty" even if the last buyer is "clean".
Secondly, tokens can remain clean, but by opening the market to external ones, there is a chance that they might never return to the platform once they are sold on an external market.

"After a liquidity event Bloomio might need to keep some cash forever waiting for a token to return to Bloomio"

Maxim Lyadvinsky (CEO)

Status Gems:
Bloomio also decided to implement a point-based reward scheme, according to which every transaction or social actions inside the platform, will allow the user to accumulate what are refeed to as "Status Gems". The accumulation of these gems will allow users to unlock premium features like the access to campaigns before the official launch, and other additional Bloomio services.
Gamification of activities can spur users not only to invest and participate more in the platform, but is can also increase the notoriety of the industry and the company itself outside the circle.
Being blockchain-based equity crowdfunding a brand new field of study and work, it is of extreme importance to find different ways to attract customers, so that they would first of all learn about this new market, understand it, and finally decide to be part of it.

4.4. Future Developments

The potential of the innovation and the presence of some favourable regulations, might make the crypto technology industry expand rapidly in the next few years. Blockchain technology is promising the creation of a market that will foster innovation and at the same time democratize the financial world, and many others together with it.
Like any other innovation though, it presents not negligible drawbacks that would have to be accessed and taken into consideration when exploring the future application of the technology, and how it will fit in the existing environment.

4.4.1. The Future of Bloomio and the Crypto Valley

The Zug canton is working constantly in order to maintain its reputation as the worlds "Crypto Valley". The ecosystem in this region is not only composed by innovative start-ups with the sole goal of making profits; but the whole community of companies and regulators, are working together to promote innovation, and create more and better opportunities. This attitude is what distinguished Zug from the rest of the regions, and it is this attitude that will foster economic and individual growth.

One of the biggest obstacle in the growth of the crypto market is and will be the regulatory framework. The relatively new technology still originates a decent level of hesitation, so it is up to regulators to adopt an innovative approach to put the minds of consumers and investors at ease. Fortunately, FINMA realizes that the chances for Switzerland to grow, are closely related to their ability to innovate; for this reason, future regulations will be developed with the goal of removing unnecessary regulatory obstacles to permit the development of new and innovative business models.
Regulatory bodies are not the only ones that have realized that the future of Switzerland and the financial environment may depend on the evolution of the Fintech industry. Start-up incubators are in fact working in order to help these new companies emerge and organize to be sustainable in the new economic environment. Start-ups are the backbone of innovation and digitalization, and it is the regulators and the incubators responsibility to cooperate in order to create an innovation and creativity friendly environment for those entrepreneurs that are courageous enough to develop their ideas.

Switzerland has been considered for quite some time now, the global centre of the financial world, and it is working toward the evolution into what will be the epicentre of Fintech innovation. This prediction is driven by the constant effort by both innovators and regulators, to foster the exploration of the new frontiers of blockchain technology.
The wide distribution of blockchain, depends on the effort innovators will make, in the adoption of the technology in already established industries, in order to show its full potential.

Bloomio is one of the first attempts to introduce blockchain technology in an industry that was already well established and structured. In the definition of the functionalities of the

platform, we can see how many of the inefficiencies usually associated with equity crowdfunding providers could be mitigated with the introduction of this innovation.
Bloomio is taking the first steps into an unexplored ground that on the other hand might provide tremendous opportunities of growth and the democratization of one of the most profitable industries in the world.

I questioned Mr Lyadvinsky on what he believes the future of Bloomio and the industry will be. What he told me was the display of the willingness of innovators like him to bring something new to the table, explore the limits of the industry, and expand as far as the company can reach to become one of the major players in the industry. Mr Lyadvinsky and its collaborators initiative, sums up the willingness to prove themselves and grow as professionals and people.
According to Mr Lyadvinsky, the creation of Bloomio and these first services provided, are just the first steps into the huge disruption that the technology will bring to the financial industry and others. The mix of this response to customer needs, and the increasing relevance of the innovation, will help companies like Bloomio become the major players in the industry of the future.
Switzerland choice of fostering blockchain-based applications and start-ups, might result to be an extraordinary decision for the future development of new and profitable industries.

When discussing the future of blockchain technology and its application in the crowdfunding industry, we need to keep in mind that just like any other innovation, it does not come without some drawbacks. All the consequences of the technology need to be accessed and kept into consideration by anyone willing to invest.

We have recently seen an increase in the number of public ICOs, which can have negative consequences with respect to the protection of the interests of consumers.
The technology allows the formation of autonomous ICOs, not backed up by any institution or platform. These ICOs constitute the majority of the ones right now in the market, and some of them have been able to raise millions of dollars overnight.
The majority of the investors in these ICOs are investing in these new tokens solely for speculative reasons, without realizing the immense risk they are exposing themselves to. The promise of a fast enrichment is pushing beginner investors to look for the next

cryptocurrency that is expected to grow fast. Their analysis is usually based solely on a poorly written whitepaper and a flashy website, and sometimes not even on that.
We have the clear example of this statement with “Doge Coin”, a fake cryptocurrency that has been developed by an Australian developer with the sole intention to prove the largely spread blind investing attitude toward ICOs. Doge Coin on January 7th 2017 has reached a market capitalization of 2 USD billion, where no project exists to back up its value.

What is important in these situations is to remind investors that behind each ICO, there is a team of people, and that a proper due diligence is necessary before deciding to invest in a new project. This is when companies like Bloomio come into play; they assess the risks, and most importantly they educate investors on the real meaning of the technology behind the crypto market.
According to Mr Lyadvinsky’s expectations, the industry will grow, and we think that blockchain-base companies will be powerful enough to substitute many of the currently available services. Consumer will become more aware of the technology and will realize the right way to use it, taking advantage of its full potential.

Conclusions

This work has been built around both the positive and the possibly disruptive consequences of the implementation of Blockchain technology in growing market of equity crowdfunding.
As we have described through this dissertation, the introduction of blockchain technology can in theory mitigate many of the inefficiencies related to the traditional methodologies of equity crowdfunding. We have also demonstrated that the actual application of the technology in a real case is possible and profitable, like in the case of Bloomio.

We have started this work by analysing the concepts behind blockchain technology, describing in details the functionalities as well as the possibilities that this innovation is able to offer. We have specifically focussed on the concept of "tokens" and the possibility of the "tokenization" of equity and assets, allowed by the technology.

Later we described the structure and the functionalities, but most importantly the limitations of equity crowdfunding platforms. Furthermore, we have illustrated how the current state of the art creates many constraints in terms of barriers to entry, security, transparency and freedom of actions, especially for possible investors.

In a following section we have analysed how the introduction of blockchain technology would alleviate many of the inefficiencies widely acknowledged in the crowdfunding ecosystem; and how the structure associated with it, has the potential to create a more transparent, safe, and decentralized environment for start-ups.
Companies looking for capital, and small investors looking for risky but profitable investment opportunities, can meet in a blockchain-based environment, with the guarantee of interacting in a safe and transparent ecosystem.

We have proposed the case-study of Bloomio, a Swiss-based company, which is currently the first entity in the world to have started working in the creation of a blockchain-based equity crowdfunding platform. This company is still working on the development of a fully functional environment, that will be perfectly operational at the end of March 2018. This new platform will allow entrepreneurs to "tokenize" a percentage of their company and sell those tokens to raise capital, through the internal secondary market.

Such technology allows for the tokenization of property and creates what are commonly known as ICOs (Initial Coin Offerings). Transactions, proofs of property, user's information, and accounts, will be all stored in a blockchain application, based on the Ethereum framework. This will grant a transparent and safe environment for both parties involved in the transactions.

The creation of a secondary market for these tokens will revolutionize the venture capital market, not only by creating a more transparent and fast way to raise capital, but will also introduce the venture capitalistic concepts into the mass market. The introduction of the technology and the tokenization of equity, permits the mass market to participate in venture capitalistic activities even with small capitals, ranging between 1000 and 20000 SFr (in the case of Switzerland).

The biggest limitation remains the legal framework which these blockchain-based companies are working in. Innovation - as it usually happens - is faster than legislation, that frequently does not allow a proper, and time-efficient introduction of the technology in the market. The Zug Canton, in which Bloomio and many others have taken office, has on the other hand realized the potential of this technology, and it is working to favour blockchain-based companies and the development of new projects.
The collaboration between the Swiss government, some independent self-regulating associations, and blockchain-based enterprises, is fostering the development of the so called "Crypto Valley", which might be the epicentre of the creation of blockchain-based applications and of the disruption of the financial system and of many industries as we know them.

References

Papers:

- (Amalar L, 2010) Lieda Amalar, Department of information System, *Managing Risks of Crowdsourcing Innovation: A Methodology,* 2010.
- (Arenas A. E., Podar M., Dalvi P., 2012) SIGSEC, *Managing Risks in Crowdfunding Platforms*, 2012.
- (Axelsson M., Knor D., Larsson W., Nydén V. Nakse N., Sorenson H., 2015) Mats Axelsson, David Knor, Willy Larsson, Victor Nydén, Niklas Nakse, Hampus Sorenson, Chalmers Tekniska Hogskola, Equity-based Crowdfunding Platforms, *Competitive situation in an emerging industry and impact on the Swedish capital market*, 2015.
- (Bakos Y., 2000) On-line Article, *The emerging role of Electronic Market place on the internet*, 2000.
- (Bellaflamme P., Omrani N., Peitz M., 2015) Paul Bellaflamme, Nessrine Omrani, Martin Peitz, Information Economics and Policy, *The Economics of Crowdfunding Platforms*, 2015.
- (Bellaflamme P., Omrani N., Peitz M., 2016) Paul Bellaflamme, Nessrine Omrani, Martin Peitz, Ifo Institute, *Understanding the strategies of Crowdfunding Platforms*, 2016.
- (Belleflamme P., 2013) Paul Belleflamme, Elsevier, *Crowdfunding: tapping the right crowd,* 2013.
- (Brodersson M., Enerbäck M., Rautiainen M., 2014) Marcus Brodersson Mattias Enerbäck Mathias Rautiainen, *Jonkoping International Business School Jonkoping University, The angel Investor Perspective on Equity Crowdfunding*, 2014.
- (Buterin V., 2014) Vitalik Buterin, White paper, *A Next Generation Smart Contract & Decentralized Application platform*, 2014.
- (Buterin V.,2017) Vitalik Buterin, Ethereum Blog, *Long-range attacks: The serious problem with adaptive proof of work,* 2017.
- (Committee on Payment and Market Infrastructures, 2017) Bank for International Settlements, *Distributed ledger technology in payments, clearing and settlement*, 2017.

- (Cresitello-Dittmar B., 2016) Ben Cesitello-Dittmar, Independent Paper, A*pplication of the Blockchain For Authentication and Verification of Identity,* 2016.
- (De Filippi P., 2015) Primavera De Filippi, Berkman Center for Internet & Society at Harvard Law, *Blockchain-based Crowdfunding: what impact on artistic production and art consumption*, 2015.
- (Deloitte University Press, 2016) Deloitte University Press, *Tech Trends 2016, innovating in the digital era,* 2016.
- (Deloitte White Paper, 2017) Deloitte White Paper, *The Blockchain (R)evolution - The Swiss Perspective*, February 2017.
- (Deloitte, 2017) Deloitte, *Blockchain: overview of the potential applications for the oil and gas market and the relate taxation implications*, 2017
- (Deloitte, 2017) Deloitte, *Initial Coin Offering, A new paradigm*, 2017.
- (Dr. Muller L., D. Meyer S., Gschwend C., Henshel P., 2017) Dr. Luka Muller, Stephan D. Meyer, Christine Gschwend, Peter Henschel, *Conceptual Framework for Legal & Risk Assessment of Blockchain Crypto Property (BCP),* MME, 2017.
- (Harmon M., 2016) Public Article, *Dictatorship, Democracy, and Blockchain*, 2016.
- (Jacobovitz O., 2016) Ori Jacobovitz, The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel, *Blockchain for Identity Management*, 2016.
- (Kirby E., Worner S., 2014) Eleanor Kirby, Shane Worner, Staff Working Paper of the IOSCO Research Department, *Crowd-funding: An Infant Industry Growing Fast*, 2014.
- (Lacasse R. M., Lambert B.A., Osmani E., Couture C., Roy N., Sylvain J., Nadeau F., 2016) Claude Couture, Roberto Genest, Francis Nadeau, Hazel de Neeve, Éric Osmani, Nicholas Roy, Jean Sylvain, International Scientific Conference on Digital Intelligence, A Digital Tsunami: FinTech and Crowdfunding, 2016.
- (Lauslahti, Mattila, Seppala, et al., 2016) ETLA Raportit, *Smart Contracts - how will Blockchain Technology Affect Contractual Practices*, 2017.
- (Lerner J., Stern S., 2014) Josh Lerner, Scott Stern, University of Chicago Press, *Innovation Policy and the Economy, Volume 14, Ch3 Some Simple Economics of Crowdfunding*, 2014.
- (Mahadevan B., 2000) California Management Review, *Business Models for Internet Based E-commerce: An Anatomy,* 2000.

- (Merton R. C., 1995) Financial Management Association International, *A functional Perspective of Financial Intermediation,* 1995.
- (Mills, David, Wang K. , Malone B., Ravi A., Marquardt J., Chen C., Badev A., Brezinski T., Fahy L., Liao K., Kargenian V., Ellithorpe M., Ng W., Baird M., 2016) Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird, Distributed ledger technology in payments, clearing, and settlement, Finance and economics Discussion Series 2016, 2016.
- (Mitra T., Gilbert E., 2014) Tanushree Mitra, Eric Gilbert, Conference Paper*, The language that gets people to give: Phrases that predict success on Kickstarter*, 2014.
- (Mollick E. R., 2013) Ethan R. Mollick, Journal of Business Venturing, The Dynamics of Crowdfunding: An Exploratory Study, 2013.
- (Nakamoto S., 2008) Satoshi Nakamoto, White paper, *Bitcoin: a peer-to-peer electronic cash system*, 2008.
- (Ohtama M., 2017) Mikko Ohtama, *ICO Smart Contracts Documentation, Release 0.1*, 2017.
- (PWC, 2015) pwc, *Blockchain - an opportunity for energy producers and consumers?*, 2015.
- (Rysman M., 2009) Journal of Economic Prospective, *The Economics of Tow Sided Markets*, 2009.
- (Schwab, 2017) - Klaus Schwab, *The Fourth Industrial Revolution,* Crown Business, New York, 2017.
- (Sehra A., Smith P. Gomes P., 2017) Dr. Avtar Sehra, Philip Smith, Phil Gomes, *Economics of Initial Coin Offering*, 2017.
- (Swanson T., 2014) Tim Swanson, *Great Chain of Numbers: a guide to smart contracts, smart property and trustless asset management*, 2014.
- (Venegas P., 2017) Percy Venegas, Economy Monitor, *Initial Coin Offering (ICO) Risk, Value and Cost in Blockchain Trustless Crypto Market*, 2017.
- (Wilson K. E., Testoni M., 2014) Karen E. Wilson, Marco Testoni, Bruegel Policy Contribution, *Improving the Role of Equity Crowdfunding in Europe's Capital Markets*, 2014.

Thesis:

- (Adiputro R. V., 2016) Ricky Valianto Adiputro, University of Twente, *Equity Crowdfunding: Signaling in European Crowdfunding Platforms*, 2016.
- (Agrawal A. K., Catalini C., Goldfarb A., 2011) Ajay K. Agrawal, Christin Catalini, Avi Goldfarb, NBER Program(s), *The Geography of Crowdfunding*, 2011.
- (Anderson P., Torstensson J., 2017) Patrik Andreson, Joel Torstensson, Chalmers University of Technology, Exploring the role of blockchain technology in Mobility and Services, 2017.
- (Baars D., 2016) Djuri Baars, University of Twente, *Toward Self-Sovereign Identity using Blockchain Technology,* 2016.
- (Bergquist J. H., 2017) Uppsala Universitet, *Blockchain Technology and Smart Contracts*, 2017.
- (Brown P. G., 2016) Paul Gordon Brown, Boston Collage Lynch School of Education, *College Students, Social Media, Digital Identities, and the Digitalized Self,* 2016.
- (Chen & Dhillon, 2003) Kluwer Academic Publisher*, Interpreting Dimensions of Consumer Trust in E-commerce,* 2003.
- (Cong L. W., He Z.) Cong Lin William, Zhiguo He, *Blockchain disruption and smart contracts*, 2017.
- (Couffinhal B., 2014) Bénédicte Couffinhal, Dublin Business School, Liverpool John Moores University, *The use of crowdfunding as an alternative way to finance small businesses in France*, 2014.
- (Czepluck J. S., Lollike N. Z., Malone S. O., 2015) Jacob Stenum Czepluck, Nikolaj Zangenberg Lollike, Simon Oliver Malone, The IT University of Copenhagen, *The Use of Blockchain Technology in Different Application Domains,* 2015.
- (Dehling S., 2013) Sebastian Dehling, Univesity of Twente, *Crowdfunding - A Multifaced Phenomenon,* 2013.
- (Eckhardt M., 2016) Marco Eckhardt, Degree Thesis, *Equity crowdfunding in Finland, an alternative investment option,* 2016.
- (Edstrom R., Pettersson J., 2016) Robert Edstrom, Jack Pettersson, Chalmers University of Technology and University of Gothenburg, *Safer smart contracts through type-driven development of smart contracts*, 2016.
- (Eotvos C. O., 2016) Csilla Orsolya Eotvos, Central European University, *Regulatory challenges in Investment-Based Crowdfunding: The model of the United States and the Lessons from Hungary*, 2016.

- (Evgenii K., 2017) Khudnev Evgenii, Lampard University of Applied Sciences, *Blockchain: foundational technology to change the world*, 2017.
- (Furnari S. L., 2016) Salvatore Luciano Furnari, Luiss, *Equity Based Crowdfunding: The Issuer Perspective,* 2016.
- (Galan M., 2016) Michal Glan, Masaryk University, *Decentralized Application Platform Ethereum*, 2016.
- (Haas P., Blohm I., Peters C., Leimeister J. M., 2017) Philipp Hass, Ivo Blohm, Christopher Peters, Jan Marco Leimeister, University of St. Gallen*, Modularization of Crowdfunding services – Designing Disruptive innovation in the Banking Industry,* 2017.
- (Harkonen J., 2014) Jirka Harkonen, Lappeenranta University of Technology, *Crowdfunding and its utilizations for start-up finance in Finland*, 2014.
- (Hass P., Blohm I., 2014) Philipp Hass, University of St. Gallen, *An Empirical taxonomy of Crowdfunding Intermediaries*, 2014.
- (Hua A.V., Noland J. S., 2016) Andres V. Hua, Jogen S. Notland, NTNU school of Entrepreneurship, *Blockchain enabled Trust & Transparency in supply chains*, 2016.
- (Jentzsch C., 2016) Christoph Jentzsch, White Paper, *Decentralized autonomous organizations to automate governance,* 2016.
- (Kikitamara S., 2017) Sesaria Kikitamara, Radboud University, *Digital Identity Management on Blockchain for Open Model Energy System,* 2017.
- (Kobbero J. C., 2014) Jens Christian Kobbero, Copenhagen Business School, *Crowdfunding - the development of an online community*, 2014.
- (Lamarque M., 2016) Mélodie Lamarque, MIT Sloan School of Management, *The Blockchain Revolution: New Opportunities in Equity Markets*, 2016.
- (Lewis G., 2009) Gregory Lewis, *American Economic Review, Asymmetric Information, Adverse Selection and Seller Disclosure: The Case of eBay Motors*, 2009.
- (Mansky S., 2016) Sarah Mansky, UC Santa Barbara, *Building the Blockchain: The co-construction of a global commonwealth to move beyond the crises of global capitalism,* 2016.
- (Mendziausyte J., Neuegebauer P., 2017) Justina Mendziausyte, Pia Neuegebauer, Jonkoping University, Financing success through equity crowdfunding, The case of start-ups and SMEs funded on an European crowdfunding platform, 2017.
- (Miller A., 2016) Andrew Miller, University of Maryland, *Provable Security for Cryptocurrency*, 2016.

- (Miller M., 1997) Mark Miller, *Computer Security as the Future of Law*, 1997.
- (Pasovs D., 2016) Dagmar Pasovs, Tilburg University Law School, *Ecquity Crowdfunding - where is the industry today?,* 2016.
- (Pilkington, M., 2016) Mark Pilkington, Université Bourgogne Franche Comté, *Blockchain technology: Principles and Applications*, 2016.
- (Rudlang M. 2017) Martin Rudlang, NTNU, *Comparative Analysis of Bitcoin and Ethereum,* 2017.
- (Schneider D.T., 2016) David Timothy Schneider, HEC Paris, *Can Equity Crowdfunding Crowd-Out Other Sources of Finance?,* 2016.
- (Sierra Mercado D., 2017) David Sierra Mercado, Master Thesis International Master of Science in Construction and Real Estate Management, *Crowdfunding, an alternative source of financing construction and real estate projects. Guideline for Developers on how to use this tool in medium size projects*, 2017.
- (Sompolinky Y., Zohar A., 2013) Yonatan Sompolinsky, Aviv Zohar, Cryptology ePrint Archive, *Accelerating bitcoin's transaction processing. Fast money grows on trees, not chains,* 2013.
- (Szabo N., 1997) Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 1997.
- (Triantafyllidis N. P., 2016) Nikolaos Petros Triantafyllidis, University of Amsterdam, *Developing and Ethereum Blockchain Application*, 2016
- (Tuning A. M., 1936) Alan Turing, *On Computable Numbers, with an application to the Entscheidungsproblem,* 1936.
- (Wessel M. E., 2016) Michael E. Wessel, Technischen Universitat Darmstadt, Crowdfunding: Platform Dynamics under Asymmetric Information, 2016.
- (Willems W., 2013) Wybrich Willems, Master Thesis Cultural Economics & Entrepreneurship, *What characteristics of crowdfunding platforms influence the success rate*, 2013.
- (Wood G., 2014) Gavin Wood, *Ethereum: A Secure Decentralized, Generalized Transaction Ledger*, 2014.
- (Zainab M. Aljazzaf, 2010) Department of computer science University of Western Ontario*, Online Trust: Definition and Principles,* 2010.

Web Articles:

- (Buterin V., 2016) Vitalik Buterin, Ethereum Blog, *Critical Update re: DAO Vulnerability,* 2016: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.
- (Coinspeaker, 2017) *Monthly Cryptocurrency and ICO Market Analysis [November 2017*], coinspeaker, 2017: https://www.coinspeaker.com/2017/12/06/monthly-cryptocurrency-ico-market-analysis-november-2017/
- (Crypto Valley, 2017) Crypto Valley Association*, Mission and Policy Framework*, 2017: https://cryptovalley.swiss/codeofconduct/
- (Crypto Valley, 2018) Crypto Valey Association, *Crypto Valley Association Collaborates with PwC strategy & on ICO Report,* 2017: https://cryptovalley.swiss/crypto-valley-association-collaborates-with-pwc-strategy-on-ico-report/
- (Dr. Diemers D., 2017) Dr. Daniel Diemers, *pwc Strategy &, Initial Coin Offering a Strategic perspective on ICO*, 2017: https://www.finance20.ch/wp-content/uploads/2017/09/20170913_Strategic-Implications-of-ICO_PwC-Strategy_DanielDiemers_vF.pdf
- (Ethereum Community. Account types, Gas, and Transactions, 2016): http://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html?highlight=gas.
- (Ethereum community. The EVM, 2016): http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.
- (Ethereum frontier guide, 2016): https://ethereum.gitbooks.io/frontier-guide/content/account_types.html.
- (Greenhalgh H., 2016) Hugo Greenhalgh, Financial Times, *Crowdfunding sites do battle with VC firms*, 2016: http://www.ft.com/intl/cms/s/0/4bf731bc2e13-11e6-a18d-a96ab29e3c95.html#axzz4BOeWyvIN
- (Howard G., 2015) George Howard, Forbes, *Blockchain Technology Is Our Chance To Rebuild The Internet In A Way That Benefits Creators*, 2015: https://www.forbes.com/sites/georgehoward/2015/08/12/blockchain-technology-is-our-chance-to-rebuild-the-internet-in-a-way-that-benefits-creators/#1a9d2ebf40ff
- (Investopedia, Hard Fork, 2017): https://www.investopedia.com/terms/s/satoshi-nakamoto.asp

- (Kocianski S., 2016) Sarah Kocianski, Business Insider, *THE EQUITY CROWDFUNDING REPORT: The democratized funding model changing the way firms raise capital - and threatening the dominance of VCs*, 2016: http://www.businessinsider.com/equity-crowdfunding-research-2016-10?IR=T
- (Lieber R. 2011) Ron Lieber, The New York Times .com, *The Gamble of lending Peer-to-peer,* 2011: http://www.nytimes.com/2011/02/05/your-money/05money.html
- (Metamask, 2017) Metamask, *Bring Ethereum to your browser,* 2017: https://metamask.io/
- (Sandner P., 2017) Philipp Sander, Medium, *Comparison of Ethereum, Hyperledger Fabric and Corda*, 2017: https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6
- (Stengel G., 2014) Geri Stengel, Forbes, *Equity Crowdfunding Targets The Gigantic Untapped Consumer Market*, 2014: https://www.forbes.com/sites/geristengel/2014/03/26/equity-crowdfunding-site-targets-the-gigantic-untapped-consumer-market/#2828ad8831e5
- (Sundararajan S., 2017) Sujha Sundararajan, Coindesk, *European Financial Regulators Warns Investors on ICO Risks*, 2017: https://www.coindesk.com/european-financial-regulator-warns-investors-ico-risks/
- (Zhao W., 2018) Wolfie Zhao, Coindesk, *Global Securities Whatchdog Worns Investors on ICO Risks*, 2018: https://www.coindesk.com/global-securities-watchdog-warns-investors-on-ico-risks/

Books:

- (Ayed G. B., 2014) G. Ben Ayed, SpringerInternationl Publishing Switzerland, *Architecting User-Centric Privacy-as-a-Set-of-Services, Ch2 (Digital Identity*), 2014.
- (Bellaflamme P., Lambert T., 2016) Paul Bellaflamme, Thomas Lambert, Emeral Group Publishing Limited, *International Perspective on Crowdfunding: Positive, Normative, and Critical Theory. Ch: An industrial organization framework to understand the strategies of crowdfunding platforms*, 2016.
- (Collen M.F., 2011) Morris F. Collen, Springer, *The Development of Medical Databases*, 2011.
- (Diadrich H., 2017) Henning Diadrich, Wildfire publishing, *Ethereum*, 2017.
- (Gorton G., Winton A., 2003) Gary Gorton, Andrew Winton, Elsevies, *Handbook of the Economics of Finance,* 2003.
- (Sterry, D. R., 2012) David R. Sterry, Independent Writer, *Introduction to Bitcoin Mining, A Guide for Gamers, Geeks, and Everyone Else*, 2012.
- (Tapscott D., Tapscott A., 2016) Penguin, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World,* 2016.

TEDx Transcription:

- (Gavers J., 2014) Johan Gavers, TEDxZug, The Four Pillars of a Decentralized Society, 2014.
- (Hoskinson C., 2014) Charles Hoskinson, TEDxBermuda*, The future will be decentralized Charles Hoskinson*, 2014.
- (Jentzsch C., 2017) Christoph Jentzsch, TEDxGraz, *The Company Which Consists Only of Computer Code*, 2017.
- (Warburg B., 2016) Bettina Warburg, TEDTalks, How the Blockchain Will Radically Transform the Economy, 2016.

List of Figures

Tables

Graphs

Figures