POLITECNICO DI MILANO

School of Industrial and Information Engineering

The age of FinTech: Providing a liquid and efficient secondary market for security based crowdfunding with Distributed Ledger Technologies.

Tutor: Prof. Giancarlo Giudici

Stefano Martinazzi Matr. 841272

Academic Year: 2016/2017

Abstract

Financial securities issued through crowdfunding campaigns suffer of many issues, mostly concerning the high uncertainty that surrounds them. Such uncertainty can be declined into several manifestations, illiquidity risk, information asymmetry between the issuer and the crowd, fair value of the value proposition and so forth. This thesis aims to understand whether the institution of a financial market infrastructure, where to trade these instruments with low transaction costs, may provide a viable solution for these issues. Taking into account the massive difference in value dealt by this industry and what concerns traditional financial markets, this work proposes the creation of a consortium composed by many crowdfunding platforms which implements a market infrastructure based upon the Distributed Ledger framework, an innovation derived from the Bitcoin's Blockchain. As results, this work proposes several possible scenarios, an original and innovative proof of concept based upon the review of literature and feedback from stakeholders and experts and some guidelines conceived with the purpose of raising the probability for the best scenario to be the future to come.

To my Mother

Index

Executive Summary

Nowadays companies are experiencing what has been called "credit crunch", since the great financial crisis of 2008 and because of the strict boundaries imposed by Basel II and, in few years, by Basel III upon the freedom for banks to lend money. Credit worthiness has become more important than ever and financial institutions developed a more sensitive risk aversion, hence many small and medium companies started not to be able any more to gain access to loans. For newly founded companies, or start-ups, the situation has become even more difficult because of their high tendency to default.

These difficulties, and the contemporary evolution of social interactions through the internet, nurtured the raise of an alternative way for raising capital, bypassing banks and financial institutions, addressing directly the crowd. Crowdfunding has been experiencing a remarkable growth being able to increase capital raised through this system several times during these few years reaching the global value of more than 30b$ in 2015. This phenomenon declined itself into several denomination of which the most attractive in terms of value committed are equity crowdfunding, where companies put shares of their equity on stake, and peer to peer lending.

The first part of the literature review, based upon Mark Saunders' "Research methods for business students" (Saunders & al, 2009), was focused upon the exploratory review of crowdfunding as a preliminary step in which the investigator acquires knowledge about the field of study, to identify the correct perspective as well as possible gaps or extensions to previous studies and spotting possible open issues to address. A promising field for debating was discovered into the security-based declination. Reducing the spectrum upon this sole denomination, it came to the surface how the issues relate to liquidity risk and information asymmetries were taken many times into consideration in the majority of reviewed papers. For profit crowdfunding or crowdinvesting is frustrated by many of the hindrances common

to traditional securities. First of all it is extremely difficult to assess the real merit of a campaign hence its fair value and “lemons” are a real problem; second crowdfunded ventures are highly risky investments and the possibilities to lose the entire commitment can’t be ignored; third once an investor commits its money to a campaign it is very impractical for his to liquidate the position because of the lack of an efficient secondary market; fourth it is very complicate for investors to control the behaviour of the backed company because of the prominent information asymmetry and the impracticability to implement corporate grade control instruments.

The following step was to push the research towards what was already envisaged by the literature as a solution for the target issues, secondary markets, enlarging the focus also towards researches concerning traditional securities. The definition of the research question concerns the possible impact upon, illiquidity, uncertainty and information asymmetries, of a secondary market, hence the author looked into the literature to search for already existing benefits of such infrastructures. This created a corollary question: “even if a financial market could be able to bring relief to these issues of our concern would be actually possible to endow the crowdfunding industry with one? Which kind of organization would be willing and capable to take the responsibility of managing such endeavour”?

The purpose of this work is to understand if said issues can be mitigated if not solved by the introduction of a liquid and efficient secondary market for crowd based securities. Independently from the response to this first question, it would be extremely expensive to set up a financial market infrastructure capable to meet all the requirements in terms of level of service for the user base and regulatory compliance. This not secondary impediment could pose an early ending to every initiative in that direction if it was not for another innovation borne in the same period by the mind of an anonymous group of cyber anarchists.

The second chapter of the thesis is focused upon the proposed solution to the question that closed the precedent paragraph. In 2009 Satoshi Nakamoto, a pseudonymous for probably a team of developers, released its Bitcoin paper and the source code on the internet and rapidly became the most successful cryptocurrency ever devised. During the last three years more than Bitcoin the financial and academic world were interested in the technology beneath it, called Blockchain, a distributed, tamper proof, censorship resistant database for recording changes of coins' ownerships. Distributed system have always suffered from issues regarding the achievement of a common consensus among all parties, which can be also faulty or even malicious, Bitcoin managed to overcome such problem, known in information theory as Byzantine General Problem, with its consensus protocol known as Proof of Work. Blockchain perform beautifully but suffers for scalability, meaning it can process few transactions per second, making it unfit for contexts that require high frequencies. Because of this limitation, the academic and corporate players took a step back from Blockchain enlarging the horizon looking at the Distributed Ledger ensemble, of which Blockchain is a sub-ensemble.

The second research topic of this work of thesis tries deeply to understand Distributed Ledger Technologies, starting from the very first principles taken from the theory of propagation of the information, from cryptograph science, game theory and economic theory. The author decided to use a particular approach dealing with this part. Because of the complexity of the topic, spawning from advance cryptography to game theory, I wanted to provide the reader with a friendlier approach allowing it to proceed one-step after another mimicking the way the author learned about it. The reader will found the chapter about distributed ledger technologies, blockchain and cryptocurrencies structured as a textbook more than as a traditional literature review. The first subchapter will cover the essential elements of a distributed ledger, for instance the meaning and differences of nodes, consensus protocols, smart contracts and so forth. The second subchapter presents the reader a collection of all the most promising distributed ledgers now available or in their pre-release phase. Thanks to what learned in the more theoretical previous part the reader should be able to understand about the main differences characterising different platforms

Then the work provides an excursus on the probable positions of several market and legal authorities about future adoption this technology on financial markets. The concluding section of this paragraph highlights the most profitable and doable implementations of blockchains and distributed ledgers in general.

The third part uses the “scenario planning” framework to answer the question: What future scenarios will be for the implementation of a secondary market for crowd-based assets built over a distributed ledger network such as this work proof of concept? To answer the question it has been used both the knowledge gathered with the literature review and the industry sentiment thanks to reports and surveys from experts and actors taken from all field of research, blockchain, crowdinvesting and concerning laws.

The fourth part presents the synthesis of what learned in the literature review in the form of a proof of concept of a distributed ledger based secondary market for crowd based securities constituted by a consortium of platform hold together by the common interest to provide the industry with an efficient and liquid exit strategy. Using flowcharts, this work recreated several dynamics we believe are compliant with all the guidelines absorbed by the literature review from all the different perspectives. The result is a public but permissioned distributed ledger, meaning every one may have a copy of it but only allowed participants can propose modifications to the record, which implements a double consensus mechanism based upon proof of work, the same as Bitcoin, and Practical Byzantine Fault Tolerant which has been used on the network of Ripple. Proof of work is the key to the creation of a clock within the system, every block is a time quantum, through solving the question the network rewards the miner with newly minted coins and this protocol promises high levels of taper resilience and censor resistance. PBFT is used to settle and record contracts among nodes, this decision take into consideration the fact contracts presents sizes and complexities significantly more important and this kind of protocol scales better for this purpose. Bitcoin’s Blockchain appears from this research to be the safest notary system ever devised, hence the crowdfunding consortium is devised to engrave the copy of the shared ledger, once every n inner blocks, on Bitcoin in order to have the maximum level of trustiness and to control that no copy of every platform diverges one from another.

Methodology

This work follows a narrative course that started from the comprehension of the crowdfunding industry, with the clear purpose to detect open issues where focusing the following analysis. The primary source of information about crowdfunding was provided by “secondary sources”. Mainly this work focused the research on academic research papers retrieved from several repositories such as SSRN, ELSEVIER and from collections of research published by Springer and Wiley. Crowdfunding is a new practice and it was preferred to rely upon reviewed material or at least contributions made for the purpose to be submit for a publication, hence for a revision. Some contribution were brought also by research from government institutions, their importance is mostly related towards understanding the sentiment towards crowdinvesting and current and future normative frameworks.

The complexity of the Distributed Ledger part imposed a thoughtful study using several data sources such as textbooks, especially for some aspects of distributed systems. Luckily, some textbooks concerning Bitcoin and Blockchains are already available with different levels of technicalities. This work retrieved many researches and papers from private enterprises such as consultancy firms and banks which were useful to understand the direction of the market’s interest but not really precise from a technological standpoint. Many primarily actors in the blockchain and DLTs environment use extensively online channels such as blogs and websites to spread information, this research used this source of information limiting its attention only to personalities of renowned authoritativeness. Whitepapers issued by developers from several different distributed ledger platforms where particularly useful in writing the chapter where was reported the current state of the competition in this field.

The novelty of this work is mainly present in the third and fourth chapters which differs greatly in the methodology chosen for each other. The difficulty for this project was the high level of novelty of both the two macro-areas of research, crowdinvesting and Blockchain, this lead to a lack of quantitative data to retrieve or even the impossibility to set up some sort of experiment to procure fresh information in the first place. This work, in order to overcome said impedances, has used the lesson gained by two articles by Omar Badreddin where it was presented the domain of "Evidence based software engineering" (Badreddin, 2013) (Badreddin & Lethbridge, 2012). Evidence based software engineering is a relatively new area of research and uses empirical studies instead of more common controlled experiments, where variability can be controlled, the complexity of the problem kept at bay and limitations in resources concealed simply by reducing the scope of the research. Bedreddin presents his EBSE tool composed by three research steps. First one is grounded theory which "is useful as an exploratory study with little or no need for assumptions or hypotheses. This method, we find, is particularly useful when the research prototype tool is at early stages of development". The second path proposed is questionnaire study by interviewing experts and potential early adopters. Third and final step is the controlled experiment. In order to understand how the future would greet a secondary market for crowd-assets based upon distributed ledger networks the author proceed with the realization of scenarios using the "scenario planning" framework which is particularly useful for project with a medium-long time horizon with a great deal of sources of uncertainties (Saunders S. G., 2009). Scenario generation is part of the set of techniques used for the qualitative research approach of Grounded theory. For the generation of scenarios this work used the framework proposed by Wulf with the aid of his "360° stakeholder feedbacks" tool (Wulf & al, 2010). Starting from what learned through the literature this work created a PEST analysis where the author collected trends, then stakeholders where asked to assess them in order to size for each one of them importance and level of certainty. The Proof of Concept is generated using a series of brief storyboards realised with flowcharts displaying several actions made by different actors, investors, platforms and depicting the underlying mechanisms put into motion by them. This part is realised from information obtained through the literature review and the third part using again information provided by stakeholders. The proof of concept provides a wide range of different situations that can be enhanced only through a secondary market and only if said market operates upon a distributed ledger network.

Conclusions

With the collaboration of several experts both from the field of crowdinvesting and from the distributed ledger one, this work was able to collect a large number of feedback concerning future trends, possible impact factors and source of uncertainties. This work defined as critical, but solid in their momentum, trends: Growing interest of institutional investors specialised in early stage financing, business angels and venture capitalists for instance; Lack of capital by banks due to the credit crunch and the poor debt rating of start-ups and SMEs; Growth of the whole fintech industry enabling more services, increasing the customer experience without sustaining prohibitively costs; The growing of the anti-establishment sentiment of millennials and digital natives can drove away millions from traditional investments' institutions. This work identified as highly impactful and extremely uncertain the regulator's actions towards both crowdinvesting and blockchain's applications. On the base of that, this work was able to find four different scenarios, among those only the best case, positive legislation towards crowdinvesting and blockchain, would have allowed the merger of the two fintech's declinations. In order to increase the probability for a fertile scenario the author proposes an original and never seen before solution based upon a permissioned consortium created and managed by crowdinvesting platforms. This solution is presented as a proof of work declined into the depiction of several crowdinvesting's usual dynamics recontextualized within a distributed ledger.

Introduction

Usually when we refer to crowdfunding, we are going to think about donations from a quite large group of people that, at best, will receive as a counterpart a token of gratitude such as a T-shirt with the logo of the project funded, a preview or something not marketable but still full of meaning.

“Simply put, crowdfunding is the process of asking the general public for donations that provide start-up capital for new ventures. Using the technique, entrepreneurs and small business owners can bypass venture capitalists and angel investors entirely and instead pitch ideas straight to everyday Internet users, who provide financial backing” (Steinberg, 2012). An indirect benefit of crowdfunding, compared to more traditional ways to gather capitals, is that success or failure of a campaign provides a direct and immediate feedback of the value proposition from a market side stand point. Crowdfunding is actually a quite old way to raise money, we could say that taxes or charity are someway a crowdfunding instance. Of course this work won’t take into consideration this kind of generalizations focusing on the

Actually, crowdfunding had not taken long before becoming a channel of investments with the purpose of obtaining a profit. This venture is commonly referred as “Crowdinvestment” and it can be declined in Equity crowdfunding, Debt-based crowdfunding, also known as peer to peer lending, and Invoice-Factoring trading. Those denominations clearly mimic the already well-established capitals’ markets but, despite this similarity, the “for-profit” crowdfunding does not share other peculiarities.

First of all the magnitudes are completely different, p2p lending accounts for 25B$ while the equity counterpart is about 2.5B$, values from 2015 (Crowdexpert.com, 2017). The vast majority of enterprises funded by this kind of operations are small or medium size enterprises (“SMEs”) and start-ups (Commission, 11/2016).

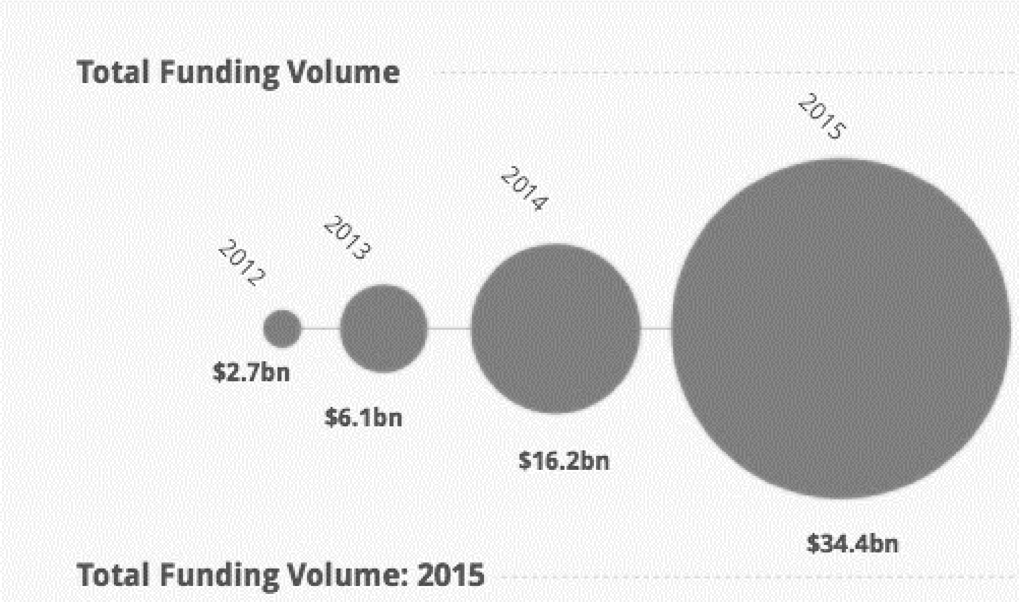


Figure 1 Global growth of crowdfunding from 2012 to 2015 (Crowdexpert.com, 2017)

Worldwide there were more than 1250 platforms for crowdfunding in 2015 according to the Crowdfund Network (CrowdfundNetwork, 2017), a number that surpassed head and shoulders what was expected a couple of years before Fig. [2].

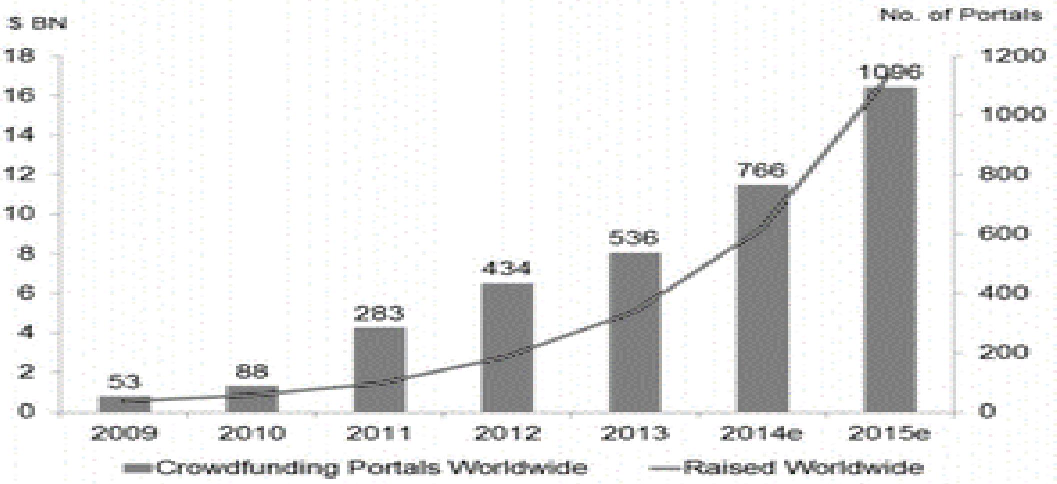


Figure 2 Actual growth and expectations in 2013 (CrowdFundBeat, 2017)

The crowdfunding market is still growing, according to the second European crowdfunding industry report crowdfunding, all denominations, grew in 2015 by 93% grasping 5.431B€ just in the European zone Fig.[3]. France, Germany and the Netherlands are the most relevant markets in absolute values while Estonia’s platforms are the biggest compared on the population size

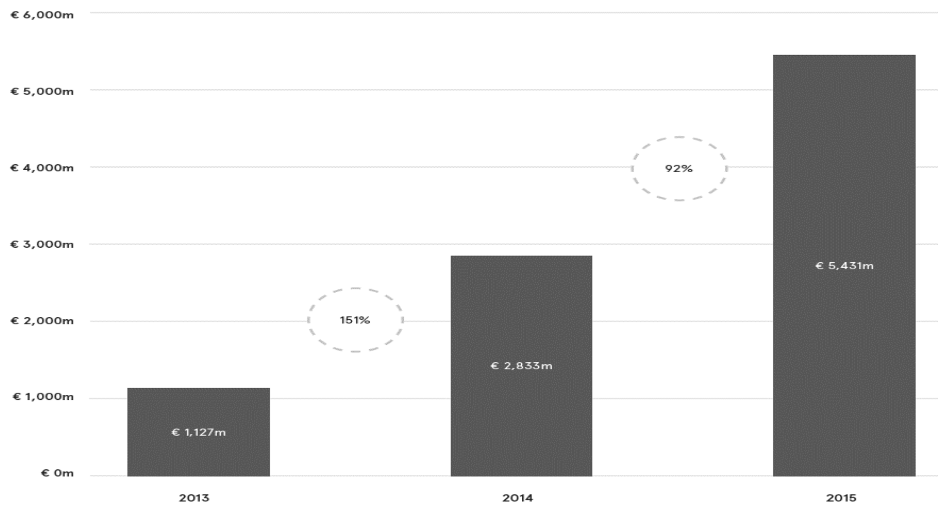


Figure 3 European Online Alternative Finance Market Volumes 2013–2015 in € EUR (Wardrop & al, 2016)

In the second European alternative finance industry report (Zhang & al., 09/2016), jointly written by University of Cambridge and KPMG, posed the united Kingdom as the predominant market for this industry with a value of nearly 4.5 billion GBP, followed by Germany, France and the Netherlands. Peer to peer lending is the richest segment but invoice trading is rapidly growing. In Europe over than nine thousands start-ups and Small-Medium enterprises where able to raise capitals with these channels. Institutional investors, such as venture capitalists, business angels or mutual funds, are showing a growing interest towards investment’s opportunities coming from these unusual, at least for them, means. The average size for an equity campaign is 459.000€.

In the first report over the Italian crowdfunding industry (Giudici & al., 2016) it has been depicted how the industry is strongly growing also in here, but with absolute volumes of a different order of magnitude.

This work aims to extend the current knowledge of the crowdinvesting by investigating the current literature, scrutinizing across several secondary sources from academic repositories and governmental reports, in order to find out open issues to address. The author will try to answer to the question of his choosing starting from a theoretical perspective and ending, if possible, with a practical and innovative, if necessary, solution.

1 Literature review

There are three different approaches towards the revision of existing literature, according to Adams and his "Research methods for graduate business and social science students", evaluative, exploratory, and instrumental. Exploratory review, used for the part interested on the Crowdfunding topic, aims to fully understand the "what is going on" within a particular field of interest, seeking new insights and issues and creating the full set of research questions. This approach will change with the introduction of the subsequent topic of interest, which is the distributed ledger technology, bending towards the descripting one in order to answer to the question "What are distributed ledger technologies and what are their actual and foreseen capabilities".

1.1 Crowdfunding and Crowdinvesting

In their work from 2015, Bouncken and Kraus gathered several definitions for crowdfunding from the literature reviewed since then (Bouncken & Kraus, 2015).

Authors	**Definitions**
(Belleflamme & al, Crowdfunding: An Industrial Organization Perspective, 2010)	*Crowdfunding involves an open call, essentially through the Internet, for the provision of financial resources either in form of donation or in exchange for some form of reward and/or voting rights.*
(Fiedler & Horsch, 2014)	*Crowdfunding comprises forms of capital supply, with which capital seeking companies publicly present themselves on specific internet based platforms to a big group of potential capital providers based on their innovative business idea and offer this group the opportunity to engage themselves with the allocation of funding* (translated from German).
(Hemer, 2011)	*Crowdfunding is a form of project and innovation funding with micropayments*
(Lambert & Schwienbacher, 2010)	*An open call, essentially through the Internet, for the provision of financial resources either in form of donation or in exchange for some form of reward and/or voting rights in order to support initiatives for specific purposes.*
(Tomczak, 2013)	*The act of taking a loan/funding traditionally performed by a designated agent and outsourcing it to an undefined, generally large group of people in the form of an open call.*

(Voorbraak, 2011)	*The process of one party requesting and receiving money and other resources from many individuals for financing a project, in exchange for monetary or non-monetary return on investment.*
(Wenzlaff & al, 2012)	*Crowdfunding is a type of fundraising for creative projects, but also for companies. Most important aspect is, that crowdfunding is open, uses the methods of web 2.0 for communication and has usually a type of material or immaterial rewarding* (translated from German).

Table 1 Several crowdfunding definitions

Starting from that collection of definitions this work also searched from the most recent ones in order to understand whether there has been some change during the last year.

Authors	**Definitions**
(Delivorias, 2017)	*Crowdfunding can be defined as an open call for 'the collecting of resources (funds, money, tangible goods, time) from the population at large through an Internet platform.* *In return for their contributions, the crowd can receive a number of tangibles or intangibles, which depend on the type of crowdfunding'. It generally takes place on crowdfunding platforms, that is, internet-based platforms that link fundraisers to funders.*
(Heminway, 2016)	*A method for financing businesses or projects that involves soliciting and securing funding from a broad, disaggregated mass of potential funders, typically through the internet.*
(Firoozi & Al, 2017)	*Crowdfunding is a practice in which start up entrepreneurs in search of funding sources may go directly to the general public (the crowd) by an internet platform to wholly or partly finance their projects.*
(Alegre & Moleskis, 2016)	*Crowdfunding is an alternative model for project financing, whereby a large and disperse audience participates through relatively small financial contributions, in a purposeful project, in exchange for physical, financial or social reward. It is usually done via internet based platforms acting like a bridge between the crowd and the projects*

Table 2 Other crowdfunding definitions

From this set of definition, it is possible to understand that crowdfunding implies a fund raising through a large number of people settled online. Another point that has been highlighted in some of the reported definitions is that crowdfunding is sometimes driven by the expectation of a reward in the future by the issuing company.

Of course, the presence of some sort of expected return implies a complete different approach towards crowdfunding introducing dynamics more relate to instruments such as debt and equity. Hence, we can distinguish a taxonomy of crowdfunding with four different branches Fig. [4]

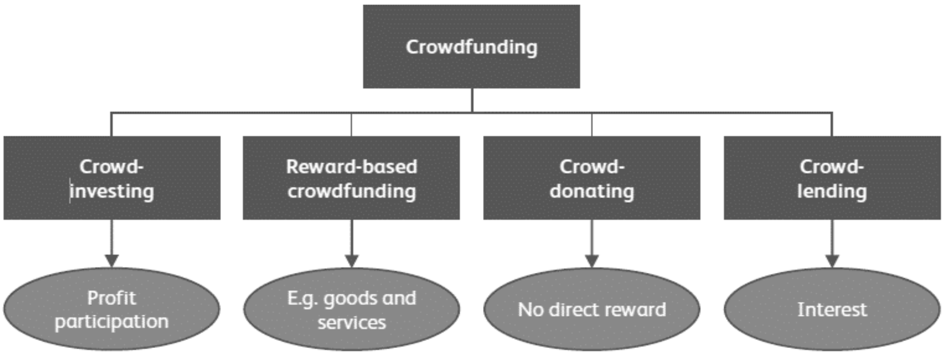


Figure 4 Types of crowdfunding and consideration for each crowdfunding category (Dietrich & Amrein, 2016)

Crowdfunding is a now quite popular way for enterprises to rise capitals during their earlier stages. This phenomenon has been placed alongside crowdsourcing, sometimes referring as an evolution of it (Benjamin & Schwienbacher, 2012). Crowdfunding has its root into the artistic field with the first website born in 2001 ArtistShare (Guan, 2016).

Crowd donating or donation based crowdfunding is the classic and oldest denomination of the group phenomenon boomed since 2009 with the platform of fundraising Kickstarter (Wauters, 2017). Indeed crowdfunding has been a valuable way for start-ups to find capitals during the shortage following the great global crisis of 2008, also thanks to the lack of regulation back then which made crowdfunding particularly appealing also thanks to the absence of costs related to the financial and not only due diligence for traditional capital queries.

Crowd investing known as equity crowdfunding, is a category where the crowd obtain pieces of the backed company ownership through receiving stocks, hence control and participation of its profits. Crowd lending or peer to peer lending does not compensate the crowd with stakes of the company but commit to release at specific moments pre-defined repayments plus interests. Invoice trading is a service of factoring where investors buy commercial credits liquidating the emitting firm.

Companies are moved towards crowdfunding for a wide range of different reasons, spawning from capital raising of course, to create a public awareness of their company and their value offer and to receive an early feedback about market appreciation of said value proposition months if not years before the actual marketization of it (Lambert & Schwienbacher, 2010). Macht and Weatherston also proposed, as a further benefit for companies that go through crowdfunding, the facilitation effect for future fund raising. The presence of a successful crowdfunding campaign has the potential to attract capitals also from institutional investors such as business angels, venture capitals or banks for loans and lines of credit (Stephanie & Weatherston, 2014).

Joachim Hemer of the Fraunhofer institute explored the industry of crowdfunding in 2011 with the major aim to understand how the phenomenon was able to help entrepreneurial ventures, who were the major players of the industry and their roles, if there were the necessity of regulation and how big was that market. Very interesting is the chapter about the description of the crowdfunding market with many visual contributions helping the reader to understand the complexity of each denomination Fig.[5] or the processes behind every campaign with a very easily comprehensible graph of the interactions of all the actors involved as in Fig.[6]. As we can see the donation based kind is the less complex of all while the equity crowdfunding is exponentially way a more complex campaign to manage. In addition, we see that banks and payments networks are involved in the process, that is because platform must have a banking licence for accepting pledges from backers therefore most of them have to rely upon escrow services provided by institutional entities or custodians.

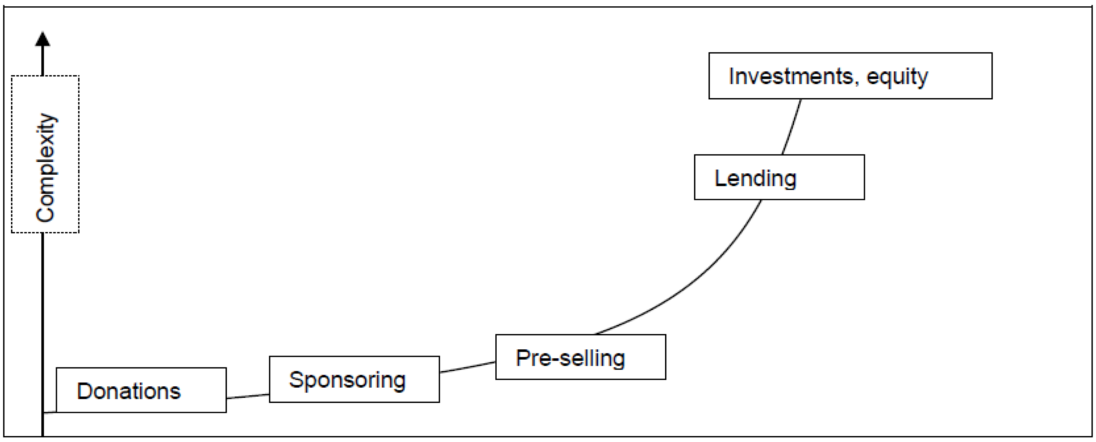


Figure 5 The major forms of capital provision ranked by process complexity (Hemer, 2011)

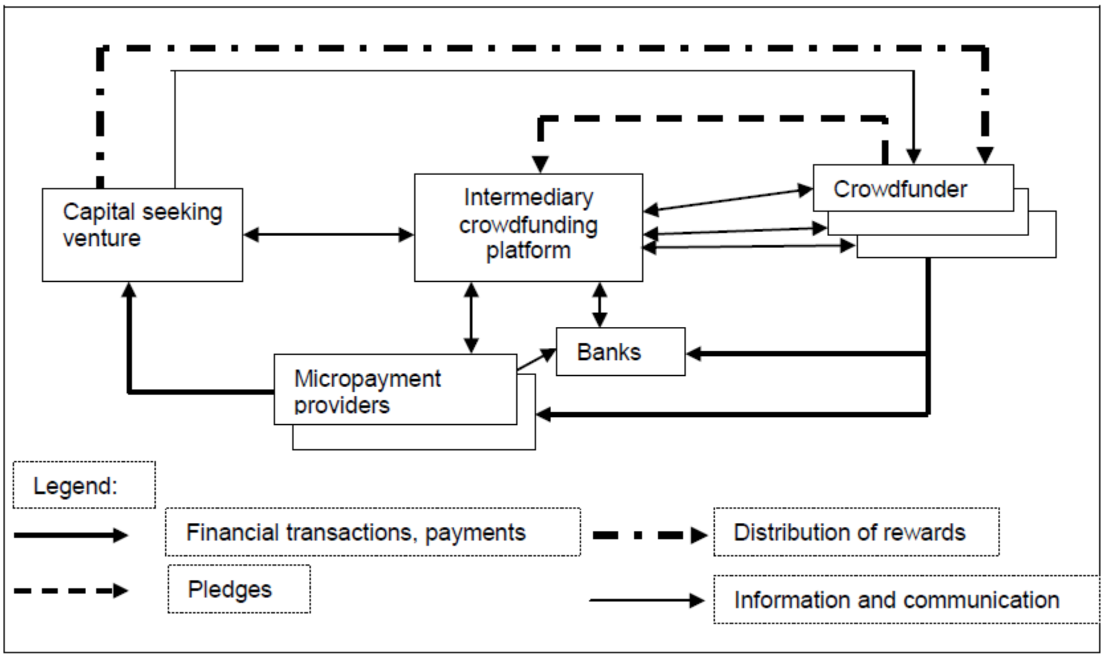


Figure 6 The crowdfunding process involving intermediaries (Hemer, 2011)

Jean Folger wrote on the website Investopedia about the high cost for a venture to campaign on a crowdfunding platform. A common fee structure account for a 5% directly to the platform plus another 3-5% to manage payments. This must be also related to the plan the platform offers, some of them let the firm holding what have been raised no matter the amount while others set thresholds beneath which the funds are returned to the crowd, less some fees (Folger, 2017).

Among all academians that studied crowdfunding perhaps the most cited are Belleflamme and Lambert. In their work about microeconomics of crowdfunding, they discovered several aspects about the contributors' side of the topic. In particular, they stated contributors are not always investors or consumers but their actions may be driven also by other intrinsic motivations, depicting crowdfunding as a true social phenomenon other than simply a financial instrument. Contributors are sensible to signals concerning the quality of the product/campaign and actions such as retaining information about equity, management composition or governance may lead to an unsuccessful campaign. The contributors are subjected to the "herd" dynamic, which basically imply that actions of contributors are consequences of the previous ones' behaviour and will be causes of the followers.

A very interesting find of this research is that the risk of frauds is actually very low; Kickstarter accounts frauds for just the 0.5% of the total number of campaigns. Likewise the previous paper also this one tackles the platform's topic. The main purpose of these is to mitigate the asymmetries in the propagation of the information ex ante, in the form of the well known adverse selection or "lemon" problem where investors may be trickled to backup campaigns not so worthy ignoring the best offers, and ex post due to the difficulties of investors to actively control the project. Platforms address these issues by bringing into the campaign also expert and well informed investors such as business angels or venture capitalists. The drawback may be a conflict of interest between the two types of investors, just because the information asymmetry is not repelled but just shifted, the crowd still may suffer it. Platform in addition, acting as trusted intermediaries, put their respectability at stake in front of the crowd therefore their interest is to control the entrepreneurs' behaviour and to pre-screen deeply every project before accepting their campaign. The paper defined this market for platforms as a winner takes all market due to the very significant presence of economies of scale and cross-side effects (Belleflamme & Lambert, Crowdfunding: Some Empirical Findings and Microeconomic Underpinnings, 2013).

In another contribute Belleflamme & all made some predictions regarding the preference of entrepreneurs towards rewarded based crowdfunding instead of the equity based one and vice versa. A lower funding requirement will concretize into a reward based campaign, in case of a high requirements, it is more likely to have an offering of equity. An offering of equity is saw in this research as a signal of a high quality project[1]. (Belleflamme & al, Crowdfunding: Tapping the right crowd, 2013)

A work of Hornulf and Schwienbacher retrieved from the "Handbook of Research on Venture Capital" studies crowdfunding, the one based upon securities emission, from the perspective of private equity. Firstly, it provides a fast recap of SEC's rules

[1] I'm not sure about this. During mergers or acquisitions the use of equity payments instead of cash is a signal of an overestimation of the value of the buyer (Hege & Lovo, 2017)

regarding investors’ protections regarding securities such as equity, debt and mezzanine. The main purpose of the paper is to discuss the similarities and the differences between private equity in the early stages of a venture and crowdinvesting. The first mismatch highlighted between the two frameworks is the ability of business angel to leverage on their contractual power to obtain from the target company tailored agreement with covenants, anti dilution agreements, liquidation preferences and so on. While the crowd usually is not able to obtain such conditions nor the actual or partial control of the company, because of the presence of hundreds of backers. This protects more the institutional investor than the crowd, but on the other side leaves the start-up with the freedom to act as they recommend. Another important difference, which plays in favour of the target company, since in many jurisdictions crowdfunding does not require the production of costly and I depth reports and due diligences. Crowds are sheltered from frauds, however, by the presence of upper bounds to the total amount of bids per project, in the U.S., this cap is one million and by the control over the platforms that act as gatekeepers. Crowdinvesting pose a threat to companies because they are forced to disclose on the platform many details about their venture, which can lead to appropriation of value by other competitors. Business angels are a better solution from this standpoint since the disclosure of sensible information is limited to few subjects that can be prevented from taking advantage from it by legal means. The authors suggest crowdinvesting is reliable just for ideas per se very difficult to replicate or that are not worth replicating in the first place. As in other works it is reported how crowdfunding benefits from the “wisdom of the crowd” phenomenon that can prevent the individual decision making bias but exposes to another one that is group thinking. Is stressed again the importance of crowdinvesting as a source of feedbacks directly from the market but the crowd is exposed to the lack of symmetric distribution of information, while a business angel is less at risk. Very interesting is the statement: “There is empirical evidence that venture capital also requires a well-developed stock market […] because venture capitalists appreciate the opportunity to exit an entrepreneurial firm through an initial public offering (IPO) […]Entrepreneurial firms that are financed via crowdinvesting are often too small for an IPO on the stock market". In their conclusions, it is also reported: "The problem is even more severe, as the crowd cannot protect itself by actively engaging in financial contracting (e.g., through covenants or staged finance)" (Hornuf & Schwienbacher, 2014).

Jack Wroldsen (Wroldsen, 2017) worked on all the different crowdfunding investment's contracts. The majority of the campaigns, 38% of his dataset, are rewarded with common shares. Common shares are granted with residual claim on profits and voting right, some of them are also protected against dilution in case of new emissions others allow the firm to repurchase the stocks for as much as the double of the paid price, hence for every share sold the firm obtain an option with a time to maturity of two years, this is of course a risk for the investor because seals the potential upper bound. The emission of preferred stocks account for the 10% of the total number. The terms for these shares varies greatly from one emission to another, some offer more protection to shareholders than the others. These forms of protection are scheduled dividend payments, shelter against dilution, buyback options in favour of investors and so on. The 8% decided to issue debt instead of equity, investors are entitled to receive at a certain scheduled period the reimburse of their loans plus interests. Another 8% put on the stake part of their future earning by sharing them with the crowd of investors. Some also are willing to set a minimum repayment threshold; in case earnings are not sufficient to reach that value, they will pay the difference with their own share. Campaigns' offers include also instruments like convertible debt, securities that pay off a fixed income for a certain timeframe until they are converted into equity, it could be both preferred and common stocks depending on what is in the agreement, and "future equity". Future equity is "something like a warrant entitling investors to shares in the company, typically preferred stock, if and when there is a future valuation event, i.e., if and when the company next raises "priced" equity capital, or is acquired, or files an IPO" (Freedman, 2017). The most interesting aspect of this paper is the complexity achievable by a single campaign. Despite the possibility to issue several options for a single campaign basically all have opted for just one kind of issuance, this may be connected to the difficulty of manage a sustainable stream of information to investors able to satisfy more than just few kind of them.

1.1.1 Legal Frameworks

Italy was the first country to adopt a set of rules for equity crowdfunding in 2013 (Consob, Regolamento sulla raccolta di capitali di rischio tramite portali on-line, 2013). For all portals is required to present formal request to be accepted in the public register of the category. For this procedure is required not to be interdicted, not to have previously been found guilty of any criminal felony concerning banking and financial activities or against public institutions and incarcerated for it in Italy and abroad, and not to have lost of honourability in other ways. After being accepted in the registry a portal must proceed toward the highest level of transparency and correctness granting equal accessibility to information to every potential or actual investor without giving misleading pieces of data or retaining crucial ones. The platform has the obligation to provide for investors also guarantying against operational risks by using just reliable and safe hardware, software and procedures for backups and disaster recovery.

In the work "Understanding Crowdfunding and its Regulations" (Gabison, 2015) the author gives a broad overview upon different legal approaches towards crowdinvesting from all the three main point of views, Platforms, Investors and Enterprises. The communitarian directives which have influences upon the industry are:"Directive 2010/73/EC (Prospectus Directive) influences how companies raise funds. Directive 2009/65/EC (Undertakings for Collective Investment in Transferable Securities Directive) influences how investment companies can raise funds. Directive 2006/48/EC (Capital Requirements Directive) and Directive 2009/110/EC (E-Money Directive) affects how crowdfunding platforms can hold funds. Directive 2011/61/EC (Alternative Investment Fund Manager Directive) can affect how crowdfunding platform function if they deal with investment companies. Directive 2004/39/EC (Market in Financial Instrument Directive) can impact how crowdfunding platform are regulated". Countries that produced their own ad hoc norms for crowdinvesting had to take into consideration what ruled by the European legislator. France requires platforms to ask for a broker licence, passing tests and evaluations by the authorities. In the UK, platforms must apply for the registry and are also abide by a “conduct of business rules…, minimum capital requirements, client money protection rules, dispute resolution rules and a requirement for firms to take reasonable steps to ensure existing loans continue to be administered if the firm goes out of business”. The paper states in Italy platforms are required for a licence as well or to operate under the shadow of a financial institution. The second part illustrates legal actions of several European countries regarding investors. Who is allowed to invest in crowdinvesting, how much a legit investor is allowed to commit in crowdinvesting overall and for a single campaign or how many campaigns a single investor may commit into? Italian ruled every campaign must be covered for at least 5% by institutional investors while UK investors must be certified or provide an auto certification of their proficiency in finance matters in order to not have limits of how much they can invest, otherwise said limit is set at 10% of the subject’s net worth. In the US, the legislator set variable thresholds depending on personal net worth. The third actor involved is the issuer that, in Italy and just for equity crowdfunding, has to be an “innovative” start-up not older than 4 years and with yearly revenues beneath 5 million €. For these companies the Italian regulator imposed a cap to how much they can rise of no more than 5 million € per year. UK and France adopted a similar solution with a cap of five and 1 million € respectively. Other rules comprise of the prohibition in the USA to trade shares before a year is passed since the campaign and the impossibilities to issue in many countries subordinated securities and hybrid instruments.

Freedman and Nutting offered an entire chapter of their book (Freedman & Nutting, 2015) to equity crowdfunding portals, the intermediaries that create the contacts between demand and offer. In the United States, under Title III of the JOBS Act, issuers cannot launch equity crowdfund campaigns without applying through a portal. Portals that performs also services of advisory and counsel, Broker-dealer, are institution registered with the SEC and FINRA and they have to perform activities of diligence like know your client processes. Portals are subject themselves to a strict auditing around their methods of assessment and picking “All intermediaries—funding portals and broker-dealer platforms alike—must conduct background checks on officers, directors, and 20 percent equity holders of each issuer, to reduce the risk of fraud. Intermediaries must disqualify an issuer if one of its officers, directors, or "participants" (such as promoters) in the offering is a "bad actor," as defined by the SEC". Moreover, portals can be held accountable for cases of frauds by an issuer, if the due diligence has not be done in a proper way, and share of the liability. Equity crowdfunding platforms receives revenues by charging issuers with a fixed entry fee or with a success fee, which is due in case the campaign reaches its goals, typically this fee is 5-10% or higher if funds raised are considerably higher than the minimum threshold. Broker-dealers can charge for their services of advisory for investors and consultancy for issuers, also they can receive funds by investors to be managed in their stead, portals not registered with SEC and FINRA cannot do wealth management services. Strategic partners for Equity Crowdfunding platforms are stocks transfer agents in charge to register every change in the ownership of a title. Escrow agents entitled to receive and hold money raised from investors until the deal is successfully closed or to refund them in case of failure, for their service they require the payment of a fee in percentage of the amount taken into custody. Platform may also need to rely upon specialized third parties for the due diligence part, charging the issuer for the service. Finally, platforms may offer the possibility for investors to buy insurances after having commit to invest in a campaign, this would hedge the risk of insolvency.

1.1.2 Issues and solutions

This work aims to understand if it is necessary to implement a structure of control over the crowdfunded start-ups in order to keep the interests aligned. The paper disposed of a survey compiled by venture capitalists, which were assumed as a good proxy of crowds involved in equity crowdfunding. From this qualitative research, the following findings were extracted:

- The crowd is highly sensible to the quality of projects' backers. Projects backed with highly competent investors will be more likely to be funded by the crowd as well.

- A pre-screening of the various deals would give a powerful signal to the crowd that the whole industry is actually well managed.
- There is a trade off on information disclosure. From one side disclosure of sensitive information may lead to an appropriation of part of the value by competitors while from the other side too much discretion about the details of a project can discourage the crowd from backing it.
- After a commitment from the crowd it has been raised the difficulty of it to maintain ongoing involvement in the project. A solution proposed would be to delegate to a third party the responsibility to protect the crowd's rights.
- In addition, this delegate should be able to sit in the company's board.

The research of McKenny and all is focused on what should be the direction of the academic interest regarding crowdfunding. As for the previous work, this one was based upon a survey spread among authorities of this field. The possible directions were catalogued into several disciplines, for instance "How do information disclosures impact the IPO process?" and "How do firms classify and characterize funds received through crowdfunding?" were disposed into the Accounting while "How does the liquidity of a secondary market for crowdfunded equities influence investor decision making?" is a possible filed of research listed into the financial file (McKenny & al, 02/2017).

Until now, every paper reviewed considered the presence of the platform as a must in order to connect the crowd and entrepreneurs. In the study "Individual Crowdfunding Practices" by Professors Belleflamme, Lambert and Schwienbacher it had been given to companies the possibility to engage the crowd with campaigns tailored better than standardized platforms would possibly be able to do. Individual crowdfunding is defined in this work as a "practices in which entrepreneurs do not make use of a structured crowdfunding platform (such as Kickstarter, RocketHub, Indiegogo, My- Major Company, Prosper) to fund their venture". In this work it has been showed how donation-crowdfunding is actually a minor part of the phenomenon accounting for less than 10%, on the other side no-profit related campaigns just the 10% of the overall population. In just one third of the cases funders are an active part, being entitled with some degree of involvement in the project, and most of this ventures are based upon individual crowdfunding. One of their findings is that individual fundraising on the average raises less than crowdfunding on platforms, also these companies renounce to the corollary visibility that a campaign on a platform such as Kickstart can bring (Belleflamme & al, 2013).

Hooghiemstra and de Buysere proposed, in their chapter from the research "Crowdfunding in Europe", the "perfect regulation of crowdfunding". Starting from what is the law as-is. Under the current European, there is no need for whoever issues securities to produce a prospectus when the value of the emission is beneath the 100.000€. In addition, there are several exceptions for particular kind of emissions that wide the cap up to 5.000.000€, over this amount the production of a prospectus is mandatory. This gap between campaigns raising between these two bounds gave autonomy to sovereign states to rule for themselves regarding crowdfunding. This lack of harmonization within the EU proved to be quite the hindrance for companies to perform cross border campaigns. This issue is present also in the crowdfunding industry where the number of cross country projects account for just the 38%, of which we should expect that a more or less large part was successfully cross border just because it had to limits their ambitions. This work urges the regulator to introduce a communitarian legislation of security based crowdfunding as condicio sine qua non to unleash its full potential within the EEA. This lack of common rules within the European market is not limited to the campaign's cap, but it spreads towards requirements for platforms in order to obtain licences, governance's structures, in particular about commitment on honesty and fairness, conflicts of interests and remuneration of the platform. From the crowd's side there might be, depending on the jurisdiction, limits for investors' commitments depending on their annually incomes, their proficiency with investments, their appetite for risk and so on (Buysere & Hooghiemstra, 2016).

Professor Schwartz published an article on the Minnesota Law Review Journal trying to address most of the scepticism from the academic world about security-based crowdfunding. The author listed three main sources of problems, which are complainant with what found in this review. The first one is uncertainty about the future of a funded firm, since the rate of failure is enormously higher in this industry than in more mature realities. Uncertainty also raises the cost of capital, which both for equity and debt is a direct consequence of risk. Second risk factor is asymmetrical information that is kept by founders, managers and other insiders but not by investors. The author states that asymmetries are even more relevant if the company deals in technology or science. It is underlined how this market failure can lead to adverse selection and morally hazardous opportunities for whoever has the knowledge. Lastly it is introduced the Agency issue, which is again a consequence of information asymmetry but kept separate by the author. Then the article reports all the different mechanisms to overcome these kind of issues, divided by Venture capitalists', Business Angels' and Regulated markets' instruments such as:

- Staged financing, which an investor, instead of funding the venture all in once the cash is delivered in several tranches conditioned each time by the achievement of some agreed milestone. This method is capable alone to address all the previously said issues. It reduces asymmetries because now founders are not incentivized to exaggerate about the potentiality of their offers, otherwise they would not be able to achieve the check points set on them, but they are not willing to "pudding the budget"[2] too much to not jeopardize their fund raising with a weak proposition. It also reduced agency costs since managers are now more than motivated to work towards the desire of the principal in order to obtain the next tranches. Finally is useful against default risk because the event may occur before the final payment, therefore just a fraction of the entire capital is lost. After having highlighted the pros of this mechanism it has also been reported how difficult such procedure would be in a crowdfunding scenario because of:

[2] An expression referred to managers who set their expectations for the future lower than their real opinion in order to raise their possibilities to outperform the budget and collect bonuses.

- Preferred stocks are shares which give the holder liquidation preference, posing them on a mid way between regular stock and debt, and that can be converted into regular ones at the holder demand. This conversion could be done as soon as the enterprise begins to grow steadily and uncertainty is lowered. This compensate partially for the lack of symmetrical information. Differently from the staged financing, this mechanism is very hard to implement because of the costs of negotiation and drafting by an attorney, expert in financial contracts, which would be considerably high in relation to a simple crowdfunding raising.
- Control Rights in order to address the agency problem. In particular, shareholders may delegate a person to seat in the board to monitor that investors' interests are protected. Same as for preferred stocks this mechanism requires very high costs because the person in charge to seat as a representative of the crowd must be payed accordingly to its preparation and position.
- Equity-based compensation for managers is a well known system of alignment for management's interests and corporate's ones. The mechanism is simply granting a certain amount of common shares to managers with the obligation to not sell them until a certain period, in order to avoid short time moves that would rapidly increase the shares' value just to dump them before the medium long term devaluation. This is a very weak tool for crowdinvesting because it is quite assumed that managers are the founders, hence they already have a relevant stake in the company's ownership[3].
- Geographic proximity is basically keeping the investments' portfolio limited to a certain area close to your HQ just to be able to keep a direct contact with the progresses of the various firms backed. Of course, this solution is not suitable for crowdinvesting since one of the main purpose of the whole framework is to break geographic limitations.

[3] It could be used as a mean to compensate external managers to take the crowd's side in the boards of several start-ups, just an idea of mine.

- Mandatory disclosure is a set of information public companies or soon to go public ones have to provide to the market and its authorities in order to be fully transparent about risks and rewards of an investment in that particular security. These documents are certified by trusted third parties with fully access to corporate information but strictly limited in communicating them to external parties by discerption agreements. The paper is highly critical about the possibilities of such a burden because of the costs connected to it.
- Appraisal and Weinberger actions are both conceived to control majority shareholders from using their powers to harm opportunistically the minority's interests. For example pushing the shares' price downward with the aim to purchase the minority's stake at an unfair price. These mechanisms are believed to potentially be applied to the crowdinvesting industry, if the value at stake is higher than a certain breakeven point.

The article then claims crowdinvesting is able to address all three key issues by using digital instruments such as the "Wisdom of the Crowd" meaning that in a vast number of investor is easier to overcome asymmetries in the distribution of the information and uncertainty. "The wisdom of the crowd is not due to some mystical phenomenon or mental convergence, but rather a simple mathematical consequence of averaging. If one person guesses too high and another too low, their average response is spot on". I would say it is an application of the law of large numbers where the information is the mean and the crowd's size is the number of trials[4]. Another Crowd-based instrument is the Crowdsourced investment analysis in which the crowd share information in order to recreate piece by piece the entire analysis of a possible target[5]. The third instrument is the reputation of founders, promoters and managers. Basically, the reputation is seen as a hostage upon with the crowd may have satisfaction in case of misconduct. In addition, a feedback mechanism can provide ex-ante a strong signal about the trustworthiness of a fund

[4] https://en.wikipedia.org/wiki/Law_of_large_numbers

[5] I don't see differences between the "wisdom of the crowd" and "crowdsourced analysis".

seeker. A very interesting tool proposed it the securities based compensation that is fairly similar to the equity based one, but instead to receive also a fixed compensation, the managers backed by crowdfunding accept to be paid primarily by the same assets they put on the market[6]. Finally the last instrument to prevent problems it the "Digital monitoring" which allows funders to verify the payments of the backed firm. In this way, the crowd is adjourned in real time about movements of the management and if they are in the direction agreed during the campaign[7] (Schwartz, 2016).

Zachary Robock from the University of Michigan raised an important issue concerning the possibility of crowdfunding to me a mean for money loundering. In the introduction to his work, he stated: "Money laundering in crowdfunding may manifest in several ways. For example, an issuer may collude with investors to exchange money for securities in a nefarious enterprise under the façade of a business transaction. […] fake investor seeking to purchase bulk narcotics (or other contraband) could crowdfund a sham company owned by a narcotics distributor. The investor/buyer would receive narcotics plus (worthless) equity. The issuer/narcotics distributor would receive funds electronically under the guise of a legitimate crowdfunding offering, which would be easier to integrate into the financial system than if the transaction were conducted in cash. A similar process could be used to funnel money out of the country to fund terrorism". The work then proceeds through a review of the title III of the JOBS Act[8], which provides to securities issued through crowdfunding to skip the Securities Act of 1933, hence less compliance work to go through for emissions equal or less than one million dollar. The second and third part of the paper analyses the role of financial institutions and crowdfunding portals dealing with money laundering. For funding portals, it is required to implement an effective customer identification program, capable to collect information about the investor, the issuer and the issuer's

[6] Of course it would be needed to have some kind of registry where all the liquidity of the company is accounted and under the control of the entire crowd. ☺

[7] Again it would be needed an infrastructure able to catch and verify all these movements ☺ ☺

[8] The American one.

directors, capable to identify cases of identity frauds and the likelihood of criminal activities. Second, a funding portal must set and maintain a system for check cash flows and identify cases of money loundering. A funding portal must always be able to answer to agencies in case of ongoing investigations. Fig. [7] shows the compliance flowchart portals have to follow (Robock, 2014).

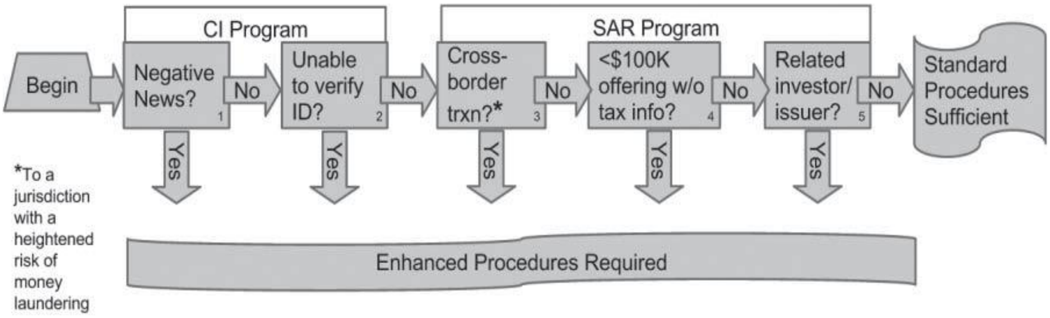

CI Program
SAR Program
Begin
Negative News? 1
No
Unable to verify ID? 2
No
Cross-border trxn?* 3
No
<$100K offering w/o tax info? 4
No
Related investor/ issuer? 5
No
Standard Procedures Sufficient
Yes
Yes
Yes
Yes
Yes
Enhanced Procedures Required
*To a jurisdiction with a heightened risk of money laundering

Figure 7 Compliance flowchart for funding portals (Robock, 2014)

Baccus and Mitteness posed the focus on the risk of Ponzi's schemes in crowdfunding projects. Ponzi schemes are frauds in which the investor is lured into investing its money on the base of astonishing return promised or actually done by the scammer. The only problem is that said returns are not the result of an occulated strategy but just a piece of the capital raised redistributed as a dividend baiting others to fell into the trap. A successful Ponzi scheme ends when the scammer understand there will be no more investors ready to give him money, therefore he will just disappear with the money that was not redistributed. Understandably, the greatest losses are suffered by the latest investors, while the earliest one possibly can really obtain a profit from the swindle. The paper takes into consideration the JOBS Act scanning it for holes in the "safety nets" proposed by that bill. In particular, they found that "Self-regulation by the crowd", "Transparency and documentation requirements", "Independent auditor reports" and "Withholding funds until financial goals are reached" are not enough to prevent Ponzi's schemes. The authors, then, proposed their own set of safe nets. First of all crowdfunding portals must go through a process of certification, in this way is defined a priori whether or not they will be able to fulfil their compliance duties. As well as for platforms also entrepreneurs willing to apply for a crowdfunding campaign have to obtain a certification (Baucus & Mitteness, 2016).

Professor Agrawal and his group studied the topic from a strategic point of view looking for evidence about the implications of geography, presence of social networks and the timing. Their research showed one main challenge in crowdfunding is the issue of information asymmetries between funders and recipients. This issue is partially mitigated by spreading information through the web and social networks and discounting feedbacks from spatially proximal funders such as family and friends (Agrawal & al, Crowdfunding: Geography, social networks, and the timing of investment decisions, 2015).

In another paper Agrawal & all pointed out the importance for crowdinvesting of being digital, therefore with a data trail behind every project: "Venture characteristics, entrepreneurial traits, investor histories, investment decisions, platform-based communications, and many other features are in these data" (Agrawal & al, SOME SIMPLE ECONOMICS OF CROWDFUNDING, 2013).

An analytical contribution of this topic was provided by a research from 2016 by Ellman and Hurkens in their working paper "optimal crowdfunding design". In their work it was showed crowdfunding, in all its declinations, may substitute or be complementary to traditional finance. Moreover, centralization of monitoring and expertise as a complement to the "wisdom of the crowd" can create even more value through economies of scale. The paper also restates the corollary benefit of gauging the market reaction to the value proposition but also, in case of a reward-based campaign also the range of the future prices, if you assume bids are actually good proxies of the value felt from the customers' standpoint. This analysis can be done by setting bid's thresholds to the campaign. Also set several rewards for diverse bid's levels allow not to hurt the company image towards early high bidders in case of the need to lower said threshold. Crowdfunding platforms are commented as vital entities since lower significantly transaction costs between issuers and the crowd acting as a trusted third party[9]. Some platforms, for instance Kickstarter, protect the crowd from fraudulent actions from the issuer such as self-funding, which could let people believe that project has more merits than the actual ones, and precludes adjustments of the bids' thresholds once the campaign has started (Ellman & Hurkens, 10/2016).

Ley and Weaven (Ley & Weaven, 2011) studied another phenomenon which is caused again by the presence of information asymmetry, the so called "agency problem" which sees the conflicts between management and shareholders feed by the conflict of interests.

I wanted to widen the research by looking for materials from non-academic entities, but still with a high degree of authority, in order to understand if their perception of the risks concerning crowdfunding is majorly limited to the area of information asymmetry or if there are other threats.

A "position paper" about equity crowdfunding issued by the Italian authority over securities, the CONSOB, raises concern about the highly illiquidity of assets issued on crowdfunding campaigns. Investors may be forced to hold their positions due to the difficulties connected to disinvestment. The absence of a regulated market for trading also prevent the definition of a market backed fair value for these assets. The paper also restates the risk of adverse selection and moral hazard (Consob, 08/2016). The lack of a secondary market and the connected illiquidity of such assets is remarked also by the European Parliament (Delivorias, 2017), by a public statement from the SEC (Aguilar, 2017) and by the Monetary authority of Singapore (Singapore, 2015).

In an opinion, paper released by the ESMA (ESMA, Investment-based crowdfunding, 2017) many of these topics where highlighted:

- "The significant potential for loss of some or all of their capital

[9] This concept will be stressed a lot ahead

- the significant risk of dilution of equity holdings through further rounds of capital raising
- the very limited possibility of liquidating an investment
- the fact that more limited information may be available about the project than would be the case for investment in a listed firm
- the potential for investors to over-estimate the amount of due diligence undertaken by platforms in relation to the viability the project;
- the potential for conflicts of interest to harm the interests of investors, in particular where the platform is remunerated by issuers, and/or projects;
- the relatively high operational risks and probability of failure of the platform itself and risk of discontinuity in the services offered that it would entail; the implications of this could be particularly significant where the platform holds client money or assets or is involved in some other way with the post-sale administration of the investment
- the potential for platforms and/or investors to exploit privileged access to the project's intellectual property".

The proposal of this paper of ESMA is to extent the already existing set of rules in the EU regarding investments, capital's markets and so forth. Also to the industry if investment based crowdfunding.

From the academic perspective, the literature review highlighted several grey point in the crowdfunding scenario, way more if we focus on the security based one. In my opinion, the most relevant one is the presence of a much skewed distribution of information between the crowd and the entrepreneur, which can lead investors towards pitfall such as adverse selection or allow fund seekers to freely do practices morally hazardous. This failure in the market can lead to fraudulent attacks such as Ponzi's schemes or disclosure of forged information. Another issue reported in literature is the risk of money laundering or financing terrorist organizations.

From this review the following research questions are done:

- How is possible to address the information asymmetry in the crowdfunding industry?
- How is possible to overcome the problem of illiquidity concerning security based crowdfunding?
- Could be possible to determine the fair market value of securities issued with crowdfunding?
- What could allow a higher customizability of Crowdinvesting campaigns?

The thesis of this work is that "an operational secondary market, upon which securities issued through equity based crowdfunding or peer to peer lending can be issued and traded efficiently would be able to provide a viable solution the just reported questions". The next part of this literature review is about benefits of secondary markets for securities.

Secondary markets are places where investors can buy and sell securities already passed through the "first issued" phase, which means securities that have already gone through a trade at least one time. For instance, the widely renowned New York Stocks Exchange or the NASDAQ are secondary markets. On the primary market on the other side, companies or governments issue stocks, bonds or other securities, for the first time and sell directly to investors.

1.1.2.1 Benefits of secondary markets

A contribution by Nassr and Wehinger tackles the advantages SMEs would benefit if their debt were marketable. In the paper, the structure of this product is the securitization of many issues of SMEs' debt into one of the categories reported in Fig. [8].

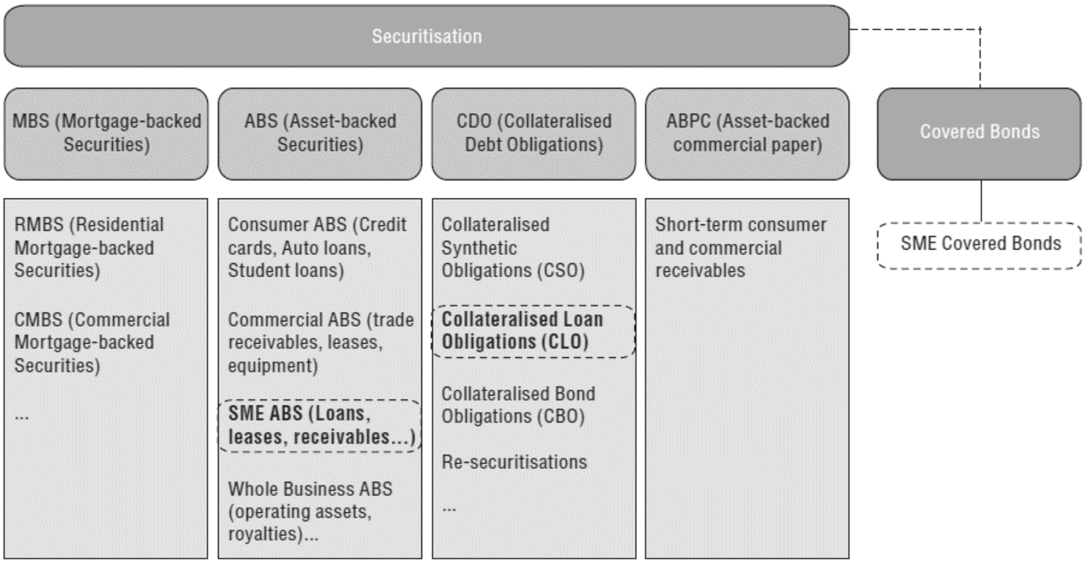

Securitisation
MBS (Mortgage-backed Securities)
ABS (Asset-backed Securities)
CDO (Collateralised Debt Obligations)
ABPC (Asset-backed commercial paper)
Covered Bonds
RMBS (Residential Mortgage-backed Securities)
CMBS (Commercial Mortgage-backed Securities)
...
Consumer ABS (Credit cards, Auto loans, Student loans)
Commercial ABS (trade receivables, leases, equipment)
SME ABS (Loans, leases, receivables...)
Whole Business ABS (operating assets, royalties)...
Collateralised Synthetic Obligations (CSO)
Collateralised Loan Obligations (CLO)
Collateralised Bond Obligations (CBO)
Re-securitisations
...
Short-term consumer and commercial receivables
SME Covered Bonds

Figure 8 Main types of securitisation (Nassr & Wehinger, 2015)

The paper displays several benefits coming from the emission of marketable tranches of debt for SMEs:

- Issuance of securities would allow the issuer to diversify its sources of capital potentially improving their financial structure through lower cost of capital and longer maturity. Also for highly risky companies, the same benefits would be achievable through cartolarisation.
- The ability to tailor their emissions on the desires of different classes of investors.
- Past issuances can be used to build a record of accomplishment of the performances of the company, improving their profile for future investors but also alongside their supply chain.
- Marketization of debt decrease the risk for traditional bank loans.

In the seventh chapter of the paper, the authors reported several difficulties and impediments for a possible securitisation of SMEs' debt. Difficulties such as the lack of economic viability of certain issuances; the presence, already stated repeatedly of a low level of information transparency and very high asymmetries. To this particular issue it is proposed that all the credit data regarding SMEs can be shared among financial institutions and/or the regulator: "Private sector initiatives may even be able to deliver such widely consolidated and standardised repositories in a more expedient manner, by refining the large amount of data already available but currently lacking standardisation, accuracy and minimum quality requirements and allowing for their meaningful use […]However, others would argue that a facility with even remotely comparable capabilities does not yet exist[10] and would take years to build, involving substantial public investment that could only be justified by the paramount relevance of the SME sector for growth, innovation and employment" (Nassr & Wehinger, 2015).

In a report of the Centre for Capital Markets (Jones & Sirri, 03/2010) Jones and Sirri assemble all the commonly recognized benefits of modern financial markets. According to the authors financial markets benefit individual investors by lowering costs related to trading, for instance is recalled how two decades ago buying twenty shares would have required a long time to process the order and cost over 100$ while modern infrastructure allows to close the deal instantaneously and for way less. Because of that, markets permit to a broader number of potential investors to place their orders and to better form efficient portfolios. Modern financial markets are essential for business to raise capitals and widely accessible capital. Markets also incorporate the maximum amount of information, giving us the best and most accurate prices.

Edmans, Goldstain and Jiang (Edmans & al, 2012) shows how financial markets are fundamentals to control the interests of management. A decrease in stocks' prices due to bad management creates the opportunity for buyers to take over the firm a change the board with people of their trust.

Vismara and Signori (Vismara & Signori, 2016) imputed the small sizes of potential free floating and restrictive regulation as a potential refrainer for the development of a secondary market. The absence of such an infrastructure cannot allow the creation of returns or to assess the potential ones.

[10] Perhaps there is something suitable

“Equity crowdfunding for investors” of Freedman and Nutting, already taken into consideration in the precedents pages, provides a couple of chapters interested about how to invest properly in equity crowdfunding. The first chapter presents portfolio strategies for investing in this kind of assets that are extremely risky, because they are shares and the issuer are private owned companies with no critical size to endure micro nor macro shocks. The reason investors would be willing to invest in such endeavours is due to the high growth potentials, hence high expected returns. Diversification is a strategy of investments which reduces risk by investing in more assets with poor correlation, meaning that causes of movements in the value of an asset as little or no effects on the value of the remaining portfolio as showed in Fig. [9].

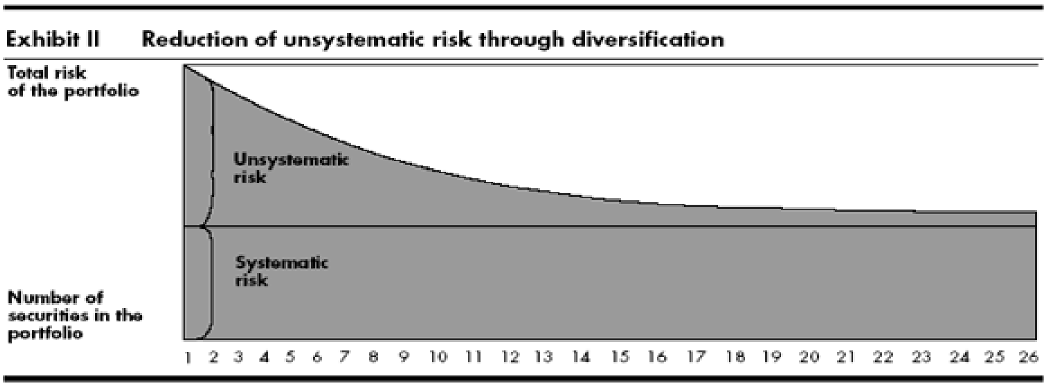


Figure 9 Reduction of unsystematic risk through diversification (Mullins, 2017)

Diversification can be achieved by investing in different issuers but also investing in different asset classes, bonds and shares are two classes of risks completely different and subject to different claims in case of default. The creation of a portfolio is also bounded to the investor’s profile, its risk appetite, its possibilities to absorb losses and its preparation about investments[11]. The creation of a proper investment portfolio is called asset allocation and it should be rebalanced periodically “Based on your asset allocation strategy, assuming you will spread your angel investments out over a few years, you should calculate how much money you can devote to equity crowdfunding investments in the current year, and roughly

[11] Those information are part as well of the Know Your Customer profiling.

how much you'll have to invest each year over the next few years..". In order to be able to allocate efficiently and rebalance periodically the portfolio it would be useful to be freely able to short assets and be able to buy securities not just during the campaign's period but there are the already many times mentioned liquidity problem and lack of secondary markets that make extremely difficult to manage a portfolio of crowd assets. Investors are forced to wait many years before being able to exit their positions through a buyback by the backed firm, an acquisition by a larger company or an initial public offer, the process of going public. The second chapter concerned about investment strategies is about the identification of suitable offerings; this can be done by indirect assessment because of the poor information available. Among these, indirect methods there are investing in companies collocated within industrial sectors in rapid and solid growth, hence using aggregate information coming from a whole segment, or by following the smart money investing where business angels and venture capitalists put their money. For investments this small, both for total and individual commitment, is unthinkable to spend money in due diligence. For a direct assessment of the worthiness of a campaign, the issuer may hire some specialised company for an evaluation and the production of a comprehensive report for the crowd. The crowd, being so large by definition, may benefit from the "wisdom" (or madness) of itself.

Economides stated a financial exchange has to be structured to maximize the satisfaction of its participants, which means minimization of transaction costs, establish the fair value of the securities traded and reduction of the risks and sources of uncertainty for investors. In this context, liquidity[12] plays a key role, because it is the direct effect of a dynamic and vast availability of offer and demand. The higher is the liquidity of the market the higher is the satisfaction. The liquidity of a market is positively correlated to the number of traders that operate on that infrastructure; hence, markets may be influenced in their values by network externalities. In the paper, it has been mentioned about two different types of

[12] "Liquidity refers to how quickly and cheaply an asset can be converted into cash. Money (in the form of cash) is the most liquid asset. Assets that generally can only be sold after a long exhaustive search for a buyer are known as illiquid" (Moffatt, 2017).

exchange. An exchange which process in real time trades is called "continuous" while ones that process batches of orders per time are referred as "call" markets. The aim of this work is to propose a mechanism to enhance liquidity by imposing "commitments to trade" and "discounts in fees" (Economides, 1993).

1.1.2.2 Initial coin Offering

This part of the literature review is going to be the trait d'union between the portion of the literature review dealing with crowdfunding and the subsequent one. Initial Coin Offers are the respective of a crowdfunding campaigns for firms that born, lives and operates on blockchains, distributed databases that use consensus protocols to reach a condition of trustless trust, meaning the correctness of what reported on the system is guaranteed by mathematical processes that bound human interests aligning them with the network's ones[13]. The greatest crowdfunding campaign ever launched was performed through an Initial Coin Offer and went under the name of "The DAO". The DAO (Decentralised Autonomous Organization) was pledge for 500.000$ was actually able to raise 150 million dollars. The DAO was conceived to become a decentralised fund of venture capital where funds would have allocated on the base of votes where the weight of each shareholder was based upon the quantity pledge during the ICO. According to its creator, Christoph Jentzsch the DAO should have been able to let contributors to maintain real time control over their funds and to completely automatize through software the enforcement of governance's rules. The DAO had been built upon an infrastructure known as Ethereum and the rights and obligations of the firm towards the pledgers and vice versa was written in the code and because of a major fault, it was possible to steal millions. Since The DAO there has been several other ICOs for other, more or less, decentralised organizations able to raise millions but academic literature has paid no interest toward them or the phenomenon and research on repositories gave no result. From material obtained from google it appears major issues are the probability for investors to be defrauded and the lack of a legal framework able to protected them and enforce their contractual rights.

[13] It will be explained way much better in the next chapter "Distributed Ledger Technologies and Blockchains"

About the second aspect, the research on Goolge presented a paper from Coinbase.com (Reuben Bramanathan, 2017) proposing a legal framework for tokens issued through an ICO. The work is divided into three parts, first one is designed to estimate how likely a particular token is to be a security under US federal securities law, the second one sets out some best practices for crowd sales and the last section is a detailed securities law analysis by Debevoise & Plimpton LLP. To understand if a certain contract can be considered a financial security the paper proposed the use of the "Howey Test" hence, in order to be recognised as a security, a contract must involve and investment in money, in a common enterprise and with an expectation of profits predominantly from the efforts of others. The proposed best practices for issuing an ICO divided in six principles:

- Principle 1: Publish a detailed white paper
  - i) Describe the protocol and the network
  - ii) Identify a clear and compelling reason for the token to exist
  - iii) Provide a detailed technical description of the proposed implementation
  - iv) Set clear expectations for total token supply and distribution
  - v) Have an independent expert review the white paper
- Principle 2: For a presale, commit to a development roadmap
  - i) Provide a detailed development roadmap
  - ii) Include estimates of time and costs for each stage of the project
  - iii) Include a breakdown of estimated expenses by category
  - iv) Allocate funding for each stage of development and consider restricting access to funding until milestones are achieved
  - v) List the names of key members of the development team and advisors
  - vi) Be transparent about remuneration paid to key members of the development team and advisors
  - vii) Quantify early contributions of members of the development team and advisors
  - viii) Between sale and launch of the network, report back to token holders periodically on progress against the development roadmap

ix) Set aside funds for independent security audits and a bug bounty program

- Principle 3: Use an open, public blockchain and publish all code

  i) Use an open and transparent blockchain

  ii) Use open source software

  iii) Where possible, commit to using standard or well-known token contracts

  iv) Do not use a private or unintelligible blockchain, or one for which the developer is the sole or primary transaction validator

  v) Commit to undertake an independent security audit before launch

- Principle 4: Use clear, logical and fair pricing in the token sale

  i) Set a maximum number of tokens to be sold in the crowd sale

  ii) Use a pricing mechanism that does not increase over time. Consider a Dutch Auction or similar mechanism to price tokens fairly

  iii) Set a cap for the amount to be raised

  iv) Set a minimum amount and refund buyers if the minimum amount is not met

  v) Denominate the price in one currency (e.g. ETH or BTC)

- Principle 5: Determine the percentage of tokens set aside for the development team

  i) Decide on the percentage of the total token supply that represents a fair reward for the work of the development team and advisors.

  ii) Release those tokens to the development team incrementally over time (contingent on their continued work on the project).

- Principle 6: Avoid marketing the token as an investment

  i) Do not promote the token as an investment that will increase in value

  ii) Promote the token based on its functionality and the use case for the network

  iii) Avoid analogies with existing investment language and processes - e.g. ‘ICO’

iv) Provide appropriate disclaimers about the token as a product, not as an investment.

The third section of the paper consists of the legal analysis by Debevoise & Plimpton LLP that concludes “Based on the above, we believe that an appropriately designed Blockchain Token that consists of rights and does not include any investment interests should not be deemed to be a security, subject to the specific facts, circumstances and characteristics of the Blockchain Token itself. Rather, given our analysis in the above, it should be characterized as a simple contract, akin to a franchise or license agreement”. Despite the fact the legal analysis gave a negative response about the effective nature of ICO’s tokens as financial contract this work will proceed on the base that it is not interested in ICOs but in crowdfunding contracts from actual platforms on blockchains.

1.2 Distributed Ledger Technologies and Blockchains

A little disclaimer: This part of the literature review will be slightly different from the previous one. During the time I am writing this chapter, I am not confident in the topic of blockchains nor Distributed ledgers, I am also strongly biased by the hype of the market carried on by several papers from consultancy groups, banks and other non academic sources. For this reason I am going to build this chapter in the same way I am learning about this topic, also to let people with solid bases in business but not so in computer science fully understand the logic behind these technologies.

In his introductory chapter Roger Wattenhofer, author of “The science of the blockchain”, states “almost all computer systems are distributed, for different reasons:

- Geography: Large organizations and companies are inherently geographically distributed;

- Parallelism: In order to speed up computation, we employ multicore processors or computing clusters.
- Reliability: Data are replicated on different machines in order to prevent loss.
- Availability: Data is replicated on different machines in order to allow for fast access, without bottleneck, minimizing latency”. (Wattenhofer, 2016)

“A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of ‘keys’ and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network” (Vaizeyv & Hancock, 2016).

Distributed ledger is therefore a shared database which ownership does not belong to a single entity, otherwise it would not be any different from a central server and its backup’s system. Distributed ledger first major use was the Bitcoin’s Blockchain. “Bitcoin has a bad reputation” this is how the Economist, perhaps, opened the “Blockchain age” with its article the 31st of October 2015 (Economist, 10/2015). If we look at Fig. [10] we can assume that the interest of the topic boomed after that article because of the palpable increment of the slope right after its publication. Days before the article nine international financial institutions joined the R^3 Cev consortium while, days later, the Linux foundation announced the launch of Hyperledger.

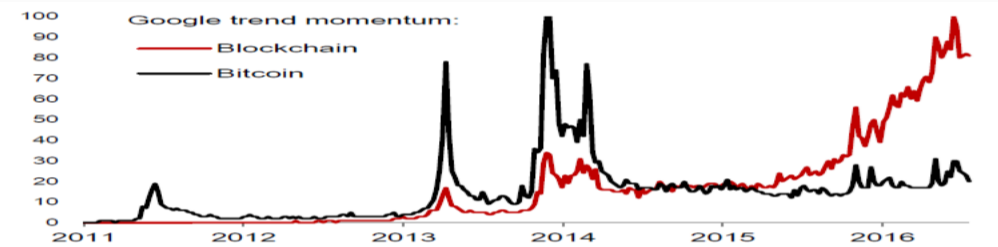


Figure 10 the momentum of interest in Blockchain compared to Bitcoin (Charles & Lunn, 2016)

Blockchain is "a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies." (Vitalik Butterin, Co-founder of Ethereum Blockchain)

The interest of the economic world around blockchain was arisen by the possibilities it was thought this technology would have allowed. In particular, source of this commotion relies on its capability to decentralise information storage and management across thousands of different memories spread all over the world without a trusted party as a central and only keeper of the validity of the system[14].

An example is a paper from Goldman Sachs entitled "What if I Told You … the Blockchain Could Disrupt … Everything". In the article, it was stated that a blockchain would have been able to make central banks retire (Boroujerdi & Wolf, 12/2015). The actual literature for blockchain depicts its range of applicability nearly as wide as the Internet itself (van der Veer & Gielen, 1/2016), there is finance of course (Biella & Zinetti, 2/2016), supply chain mgmt. (Ream & al, 2016). , IoT (Dorri & al, 9/2016), policy makers (Condos, Sorrell, & Donegan, 1/2016) and many others (Donkers, 2016) (Krawiec & al, 8/2016) (Groarke, 8/2016). From Fig.[11] we can see the perception of the applicability of Blockchain.

[14] Today the vast majority of centralised or decentralised databases has to submit to the rules of its administrator, banks, central governaments and so forth

At this point an initial fair question should be: “What is in reality a Distributed ledger or a Blockchain or a Cryptocurrency?” Another interesting question could also be “Everything they said about those technologies is true or is partially biased by the hype?”

I shall start from the first question introducing this fascinating topic from a scientific and technical stand point, from an economical one and finally from a regulatory point of view.

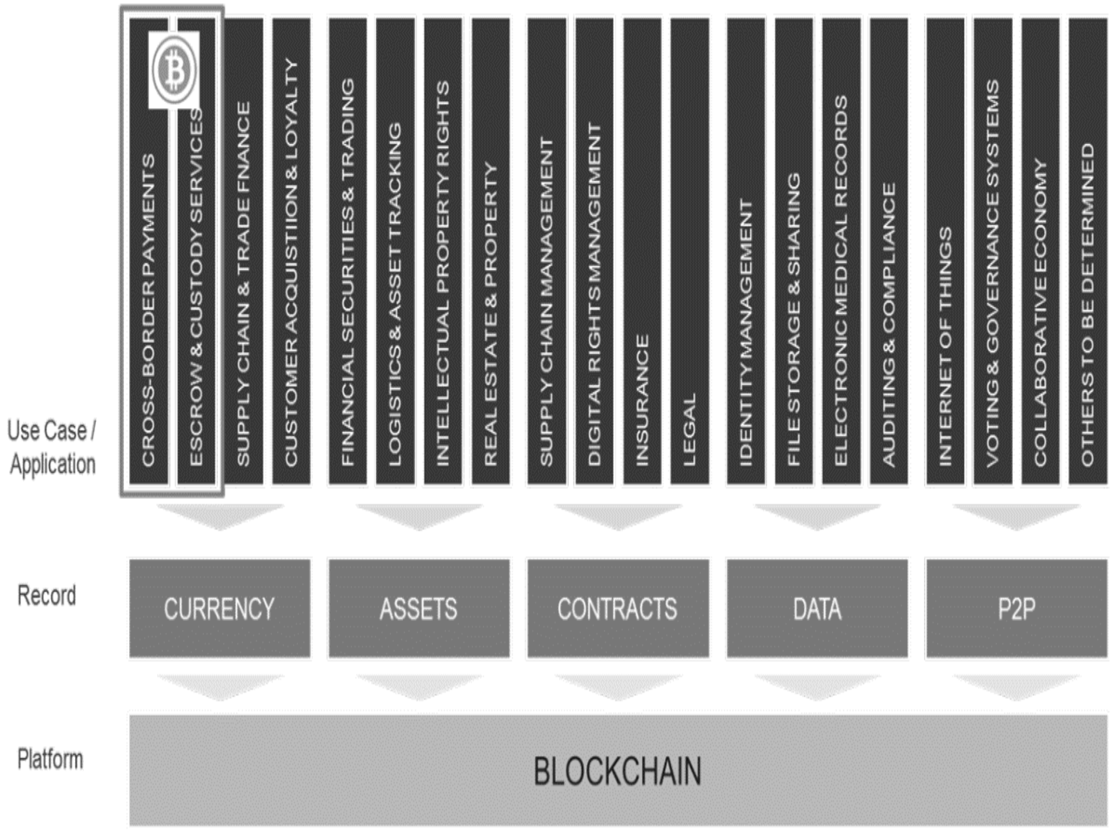


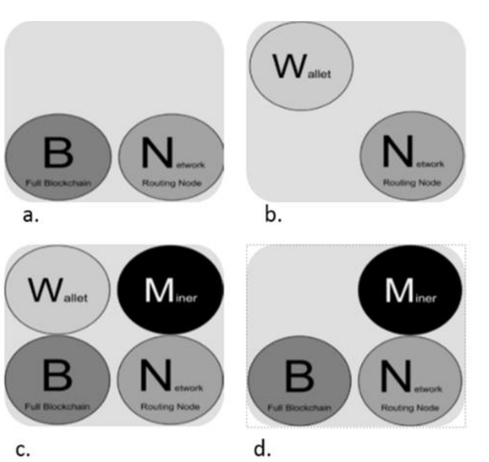
Figure 11 Several applications based on Blockchains, (Morgan, 01/2016)

1.2.1 Nodes

“We call a single actor in the system node. In a computer network, the computers are the nodes, in the classical client-server model both the server and the client are nodes, and so on. If not stated otherwise, the total number of nodes in the system is n” (Wattenhofer, 2016).

Fig.[12] Any computer that connects to the Bitcoin network is called a node and every one run on the same set of “consensus rules”. Changing a rule can be done through a “Fork” meaning that a new currency is created from the last block collectively accepted. Fork because it might be that not all the network is agreeable with the new set of rules and decide to go on with the old one, creating a fork (Unknown, Full Nodes, 2016).

Figure 12 Several types of nodes



There are basically two types of node, full nodes (a.) and lightweight nodes (b.). A full node has the whole blockchain stored in its memory (to date 60Gb) and they are in charge to check new blocks are compliant with the rules The full blockchain node relies on the network to receive updates about new blocks of transactions, which it then verifies and incorporates into its local copy of the blockchain. They are considered the “Backbone” of a blockchain. The most implemented version of full node (for bitcoin) is the “Core” or “Satoshi client”(c.).Not all nodes have the ability to store the full blockchain. Many bitcoin clients are designed to run on space- and power-constrained devices, such as smartphones, tablets, or embedded systems. For such devices, a simplified payment verification[15] (SPV) method is used to allow them to operate without storing the full blockchain. Some full nodes also carry on the mining protocol, the addition of a new block to the blockchain hoping to be rewarded (d.) (Antonopoulos, 11/2015).

[15] It is descripted in the Chapter “Bitcoin”

1.2.2 Shared Ledger

A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. (Vaizeyv & Hancock, 2016)

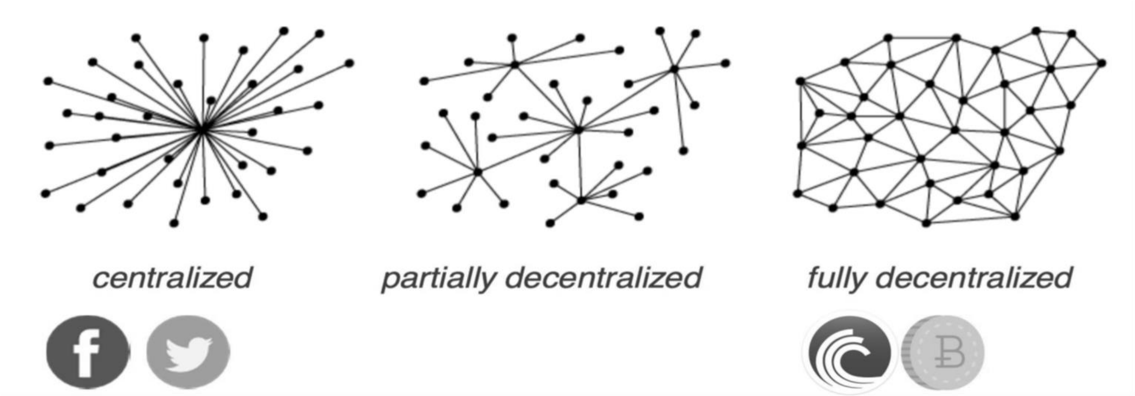


Figure 13 An exemplificated schematic of a centralized, a partially decentralized and a fully decentralized network (Grant, 2016)

Fig. [13] shows how are managed interactions between different nodes moving from a Master/Slave framework towards a peer-to-peer one. Tab. [3] from an online article reports the main differences between the two vertices *(Symbiont, 2017).*

Table 3 Distributed Vs Centralized Ledgers

Distributed Ledgers	Centralized Ledgers
Consensus on Data	Internal and external reconciliation
Immutability	Corruptible
Distributed	Single point of control
Peer-to-peer	Gateways and middlemen
Cryptographic verification	It can be implemented
Cryptographic Authentication	Actions are done on behalf of others
Resiliency and up-time increased by size	Limit number of back-ups

There are four important benefits of distributed ledger technology accordingly to the report from the UK technological commission:

- Reconciliation through cryptography: Institutions such as banks or governments currently send messages to each other in order to communicate details of transactions. It is up to the receiver then to update its copy of the ledger to the new version. This process raise concerning about the authenticity of the sender and the matching of the two copies of the ledger after the update. Bitcoin's distributed ledger provided a possible solution to these two issues by implementing into the said process mathematical functions used in modern cryptography.[16]

- 2) Availability of many copies: This lowers significantly the chances to have failures in the system due to the presence of many control points. Institutions would be spared from the burden to duplicate and maintain their back-ups. Finally, the up time of the overall system is enhanced due to its level of redundancy.

- 3) Granular access control: "Distributed ledgers use 'keys' and signatures to control who can do what inside the shared ledger. These keys can be assigned specific capabilities only under certain conditions. For example, a regulator may have a 'view key' that allows it to see all of an institution's transactions, but only when a key owned by a court gives it permission (control) to do so".

- 4) Granular transparency and privacy: Because of the use of cryptographic instruments and massive redundancy, as stated in points 1 and 2, some distributed ledger systems have the properties of being nearly irreversible to prevent tampering with previous transactions[17] (van Oerle & Lemmens,

[16] This topic will be explained thoroughly in the Consensus and Bitcoin's chapters

[17] In my opinion the "irreversibility" part is not a core property of a Blockchain, an example was the hard fork made on the Ethereum Blockchain, after a cyber crime made 60 m$ worth of Ether (another digital coin) disappear, with which the history after the illicit event was erased from the blockchain and the situation before it was restored. Also it would be possible to implement into the

> 2016). “This allows a regulator or an independent body such as the judiciary to see with confidence that the contents of a database had not been edited or modified in any fraudulent way. Given the right conditions, it also allows them to unlock records that would otherwise be completely private and un-viewable. This could be useful for businesses (e.g. banks) in their regulatory reporting, fraud prevention, and could even empower citizens to hold the government to account”

The academic literature posed strong boundaries in the world of distributed systems, hence also for blockchains and distributed ledgers. The CAP Theorem from Brewer posed three main features of distributed systems in mutual trade off. These are Consistency which is basically as every node has the same dataset in every moment, just like they were a single node, Availability that implies that every request received by a non faulty node must end into a response and Partition Tolerance that allows the network to fully work even if a number of massages are lost (Gilbert & Lynch, 2002).

Another bound proposed by Trent McConaghy (McConaghy, 2017) is the DCS triangle that again puts three dimensions in trade off, even if this is an engineering bound, not a fundamental one like the CAP theorem. The three dimensions are Decentralization, which means no node has a higher degree of control on the network, Consistency like the CAP and Scalability to allow the network to maintain an acceptable level in its performances even if the size of it increases. In Fig. [14] it is reported the DCS triangle.

code that a particular node (ex: the FED or the BCE) may change the Blockchain freely. EVERYTHING depends on what is written into the code.

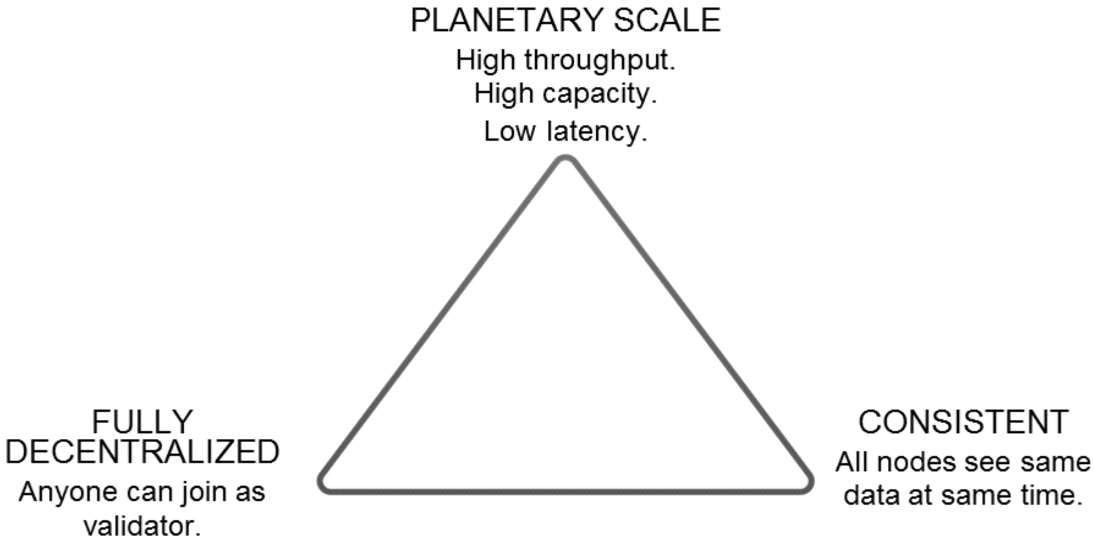


Figure 14 DCS Triangle (McConaghy, 2017)

As mentioned all these components are in mutual trade off therefore every system may move towards mixed solutions choosing locally second bests just like in Fig.[15]

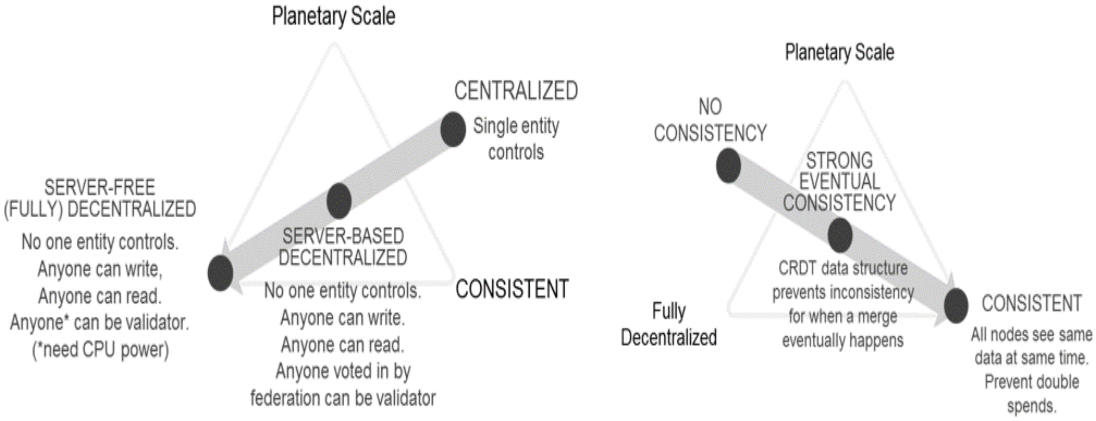

Planetary Scale
CENTRALIZED
Single entity controls
SERVER-FREE (FULLY) DECENTRALIZED
No one entity controls.
Anyone can write,
Anyone can read.
Anyone* can be validator.
(*need CPU power)
SERVER-BASED DECENTRALIZED
No one entity controls.
Anyone can write.
Anyone can read.
Anyone voted in by federation can be validator
CONSISTENT
Planetary Scale
NO CONSISTENCY
STRONG EVENTUAL CONSISTENCY
CRDT data structure prevents inconsistency for when a merge eventually happens
Fully Decentralized
CONSISTENT
All nodes see same data at same time.
Prevent double spends.

Figure 15 DCS Triangle trade off (McConaghy, 2017)

I would like to stress the fact that a shared ledgers is not yet a Blockchain but just its upper layer, like Blockchain is not Bitcoin, I felt like to remark this concept because during my research I growth the conviction that there is a lot of confusion about the different technological boundaries.

I thought that something like Fig.[16] could help. We can see how a distributed ledger has to be first of all distributed among more data storage supports, then if more than a few chosen people may have access to the data saved in there we have a “public shared ledger”, then if anyone is able to make modifications to the ledger, through a trustless consensus protocol, we have an unpermissioned, public shared ledger.

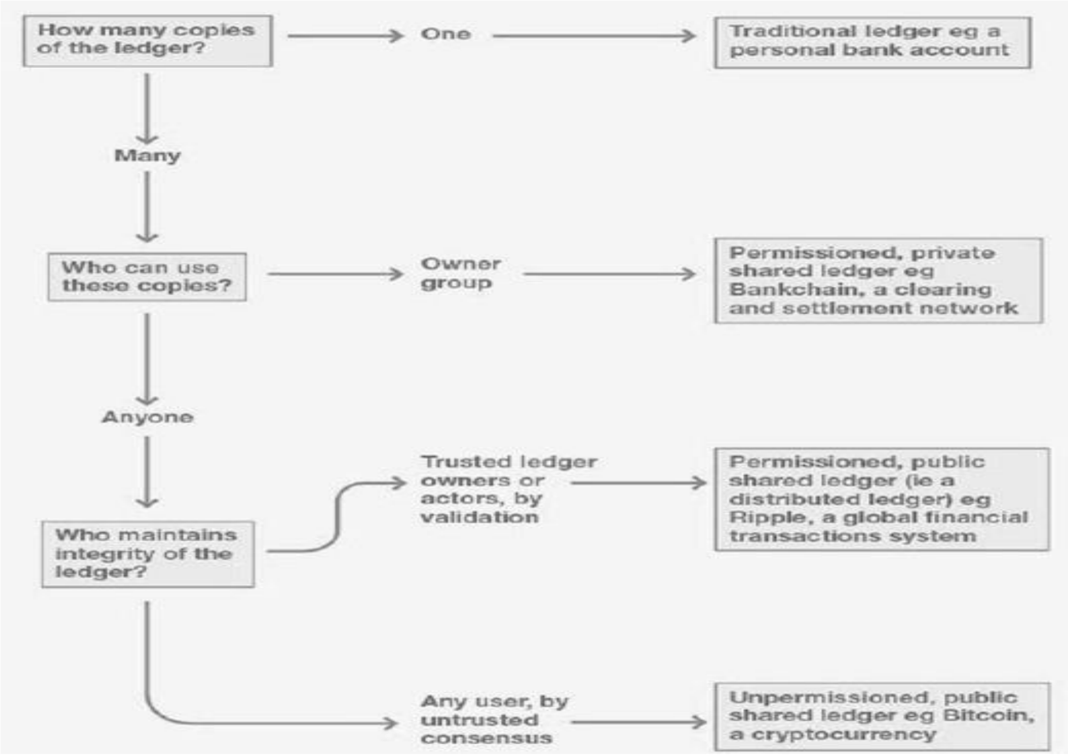
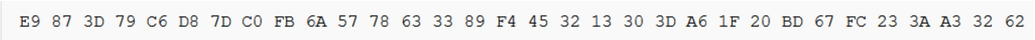

How many copies of the ledger?
One
Traditional ledger eg a personal bank account
Many
Who can use these copies?
Owner group
Permissioned, private shared ledger eg Bankchain, a clearing and settlement network
Anyone
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger (ie a distributed ledger) eg Ripple, a global financial transactions system
Who maintains integrity of the ledger?
Any user, by untrusted consensus
Unpermissioned, public shared ledger eg Bitcoin, a cryptocurrency

Figure 16 Dave Birch, Distributed Ledgers Taxonomy, Hyperion Consult

1.2.3 Cryptography

In Bitcoin’s ecosystem an account is usually referred a “wallet”, from a wallet Bitocins may flow out of go into it. Everyone who knows the “address” of a wallet may make deposits into it but only its owner, or whoever knows its “private key”, may do transactions from it to another wallet. A wallet is nothing more than an encrypted file that contains a number of private keys. The private key is a string of characters, in Fig [17] a 256-exadecimal example of a key, of course since the knowledge of a private key allows to withdraw coins from a wallet it must be kept secret.



```
E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62
```

Figure 17 Private key, example of a Private key, https://en.bitcoin.it/wiki/Private_key

The Public key is a code mathematically related to the private one in an "only way" sense, this relationship is at the base of an "Asymmetric Cryptography" protocol because from the private is possible to generate a public but the vice-versa is not possible (trapdoor one-way functions[18]). Fig[18] shows the logic of an asymmetric cryptography, in particular Bitcoin uses the Elliptic Curve Multiplication.

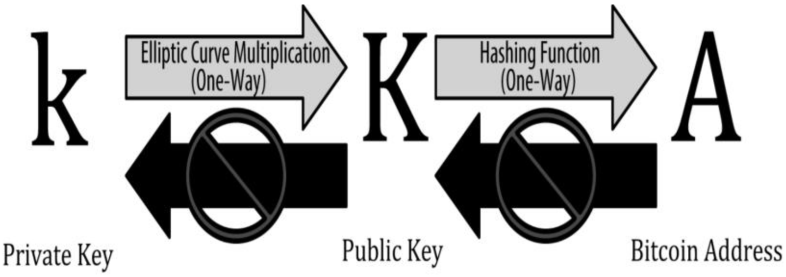

k
Elliptic Curve Multiplication (One-Way)
K
Hashing Function (One-Way)
A
Private Key
Public Key
Bitcoin Address

Figure 18 One way trapdoor function, Mastering Bitcoin, A. Andronopulos

1.2.4 Transactions

A transaction is the change of ownership of a physical or not physical good; we could define the most basic transaction with just three pieces of information, the previous owner, the new owner and the underlying good.

Transactions of Bitcoins start with the two parties announcing the change of ownership of a certain amount of the underlying; this announcement has to be validated by the presence of the digital signature of the previous owner and the indication of the address of the new one.

In the Bitcoin's blockchain, a valid transaction is recorded, with several others, in a new block that upgrades the account positions of the two parties on the shared ledger.

[18] A one-way function is a mathematical function that is highly asymmetric in terms of its computational complexity with respect to its inverse function. Such a function is easy to compute in the forward direction but diabolically difficult to compute in the inverse direction. Such functions are based on *hard* mathematical problems, such as factoring large composites into prime factors, the discrete log problem, and the knapsack problem (Thorsteinson, 8/2003).

1.2.5 Consensus

In the shared ledger’s paragraph, I introduced the term “consensus protocol” as a mechanism to avoid the presence of a trusted third party as the validator of all the transactions, which is how the banking and payments systems currently do, as showed in figure [19]. In the situation depicted two entities, the cardholder and the shop, which do not know or trust each other have to directly rely on at least three trusted third parties to be sure that the transitions will be fully legit. The cardholder has to send the request of payment to its bank. The bank before confirming the cash transfer, must verify the account of that entity has the availability of the amount requested. The bank send the data through the payment circuit, MasterCard in this case, to the shop’s bank which confirm the reception of the due and both, the seller and the buyer banks, upload their clients accountant situations. This system can make all the parties to be sure about their financial positions and prevent anyone from spending more than what is allowed to.

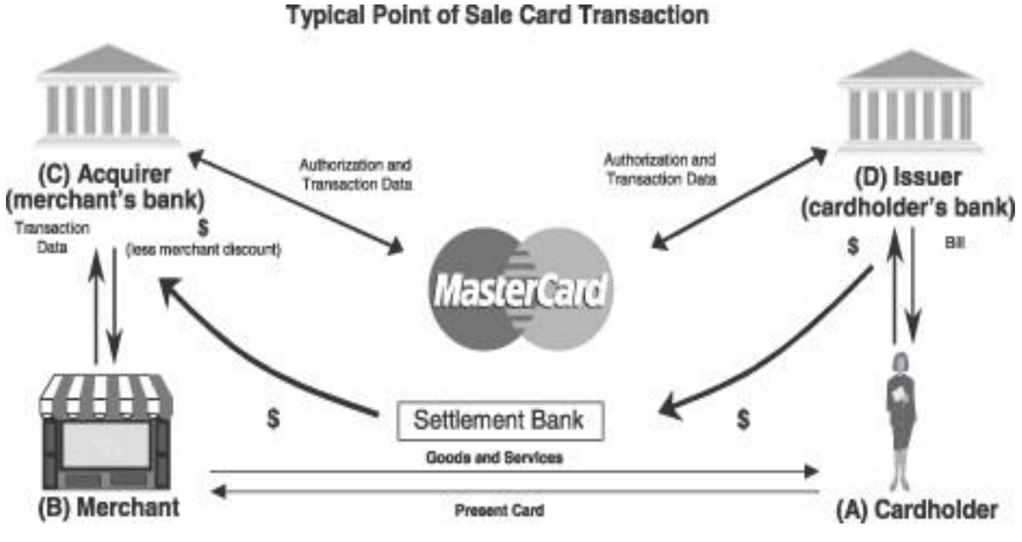


Figure 19 Darragh O'Grady, Digital Currencies & The Future Role of Banks, http://www.dappsinfintech.com

During the transaction depicted, the two parties had to rely upon three other entities, two banks and the payment system. Those three “super partes” entities facilitated the transaction because, while the shop may not trust the shopper, they trust each other and are able to reach consensus quite easily. Another very important point is that that at the end of the transaction the three parts upload their ledgers in a private way without having in common any information.

For a distributed system with hundreds or thousands different nodes and a single ledger consensus must be obtained through more complex means, these means are called “Consensus Protocols”. I decided to investigate deeper into this part of the introduction because consensus is the key point of Bitcoin and any other decentralised system, and most of the characteristics of a decentralised platform depend on the consensus protocol integrated (Shi, 2016).

The necessity of these protocols are due the presence of three related issues: byzantine generals’ problem, interactive consistency and Consensus.

1.2.5.1 Consensus and agreement algorithms

A city is under siege by Byzantine General and its army composed by several divisions, each of them commanded by a lieutenant, camped outside its walls in different locations, can explain the “Byzantine Generals problem” Fig. [20].

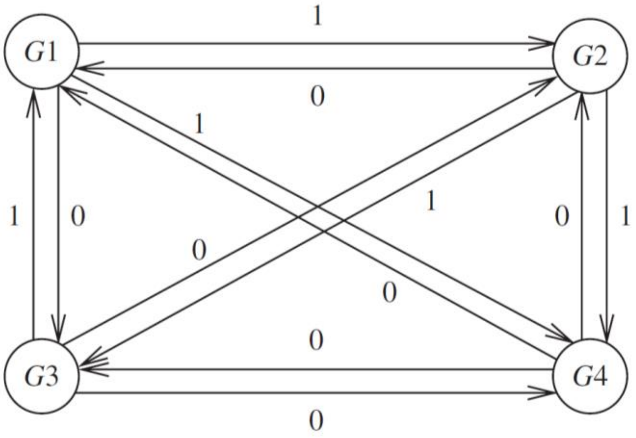


Figure 20 Byzantine generals sending confusing messages. (Kshemkalyani & Singhal, 2008)

The general and each division lieutenant may communicate with another only by messengers. The commanders have to convey on a common strategy, attacking all together at a certain moment or retreat from the siege. The problem is there might be some treacherous general among the army who can prevent the group from reaching the agreement. The Generals must be sure that A: all the loyal commanders decide upon the same plan and B: the number of traitors is not enough to jeopardize the strategy (Lamport & al, The Byzantine Generals Problem, 06/1982). Following the reading of my choose (Kshemkalyani & Singhal, 2008) I shall make a little bit of introduction to the issue. “Formally, the difference between the agreement problem and the consensus problem is that, in the agreement problem, a single process has the initial value, whereas in the consensus problem, all processes have an initial value. However, the two terms are used interchangeably in much of the literature and hence we shall also use the terms interchangeably”.

In distributed systems, failures may be both unintentional, like a downtime of a node, and arbitrary, like in the Byzantine problem. Distributed systems may also be synchronous, therefore a failure in sending a message is detected in the very moment by all the system, or asynchronous, if the time window is not wide enough there is no way to understand whether the missing message is due to an high latency or a failure. Messages can be passed through the network from and to any node. The receiver of a message knows for sure which node sent it, i.e. is not possible for the node j to send a message to node k pretending that message was sent by node i. Only the nodes may be faulty the channels cannot. Messages may or may not be authenticated, meaning that if a node is sending a message it received from another, if it has been signed, we are sure that it was really received and then sent again, i.e. i receives a message from k; k states that message was sent by j and on the message there is the signature of j, which is not possible to be forged by k.

In the case of a distributed ledger platform we may assume that we are in an asynchronous scenario, as stated in this very recent paper (Pass & al, 08/2016): “Assuming a synchronous network, however, is a very strong, possibly unrealistic assumption; indeed, Nakamoto's protocol is explicitly designed to work in a network with message delays, and indeed is executed on such a network (i.e., the Internet)”.

Any algorithm solve the consensus problem only if complies with three requirements:

- Termination: Eventually each correct process sets its decision variable.

- Agreement: The decision value of all correct processes is the same: if pi and pj are correct and have entered the decided state, then di = dj (I, j = 1, 2,…,N).
- Integrity: If the correct processes all proposed the same value, then any correct process in the decided state has chosen that value.

The consensus problem differs from the Byzantine one since each node has an initial value and all the non faulty ones must convey on a single value, from our perspective all nodes must agree on the new state of the public ledger. This change a little the conditions for a proper consensus protocol:

- Termination: Each non-faulty process must eventually decide on a value.
- Agreement: All non-faulty processes must agree on the same (single) value
- Integrity: If all the non-faulty processes have the same initial value, then the agreed upon value by all the non-faulty processes must be that same value.

The interactive consistency differs from the Byzantine problem since each vertex has an initial value and at the end of the round all non faulty process must convey upon a vector of values, with one value for each point.

- Agreement: All non-faulty processes must agree on the same array of values A[v1… vn].
- Validity If process i is non-faulty and its initial value is vi, then all non faulty processes agree on vi as the ith element of the array A. If process j is faulty, then the non-faulty processes can agree on any value for A[j].
- Termination each non-faulty process must eventually decide on the array A.

These three problems are proved to be equivalent, meaning that a solution for one is also a solution for the other two (Cachin & al, 2001).

In 1985 Fischer, Peterson and Lynch demonstrated it was impossible to reach agreement in an asynchronous distributed system, this result is recalled as the FPL impossibility, (M. J. Fischer, 1985). This limit has been circumvent by using solutions of second best like sacrificing determinism for probabilistic algorithms, or adding time to the model increasing the time frame, I would here recall the 10 minutes block timer in the Bitcoin blockchain, enrich the model with an oracle or weakening the conditions of agreeability (Correia & al, 2011).

Oracles are trusted entities signing claims about the state of the world. The oracle in this case is a failure detector. Thomas Bertani CEO of Oraclize wrote: “To us an oracle is a third party you have to talk with when you need some data you don’t want to (or you cannot!) fetch by yourself. The reasons for this can be many. […]To make this more general, we can define three entities: data-source; query; the oracle/oracle network. As for the data-source, this is the source of the information you are looking for, this can be anything depending on your actual query, some examples can be “Augur” (while looking at future events/facts), “Bloomberg” (while looking for financial data), “Bitcoin blockchain” (while looking for an address balance, a given transaction OP_RETURN content or any other blockchain data), “WolframAlpha” (while looking for the response to a given Wolfram Alpha query). The query is a formula the data source you have chosen can understand in order to give you back the data you want. The oracle/oracle network is the party in charge of connecting you to the data-source (Bertani, 2017). Like in Fig. [21].

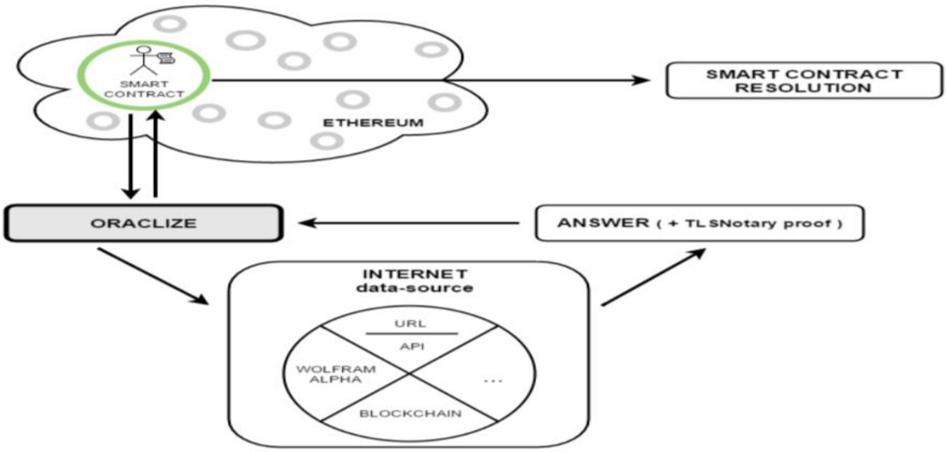


Figure 21 Oravlize approach towards feeds for smart contracts (Bertani, 2017)

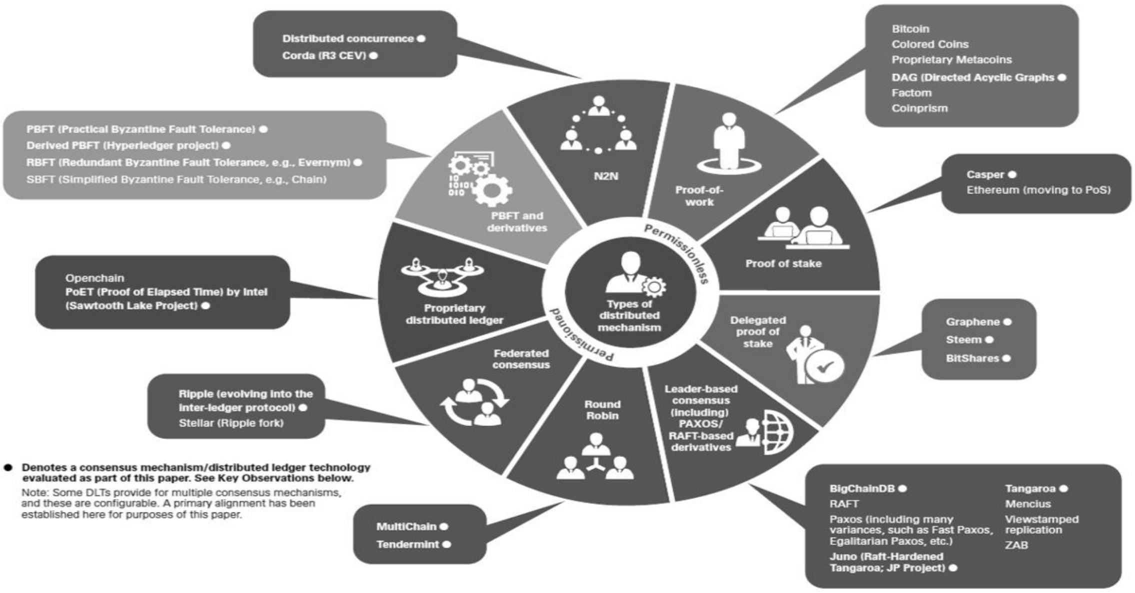
From the figure above, it is evident how a system that is supposed to be distributed and trustless is actually relying upon a controlled source of information, therefore weakening if not disrupting the nature of a blockchain. If the data feeder is not honest, it could be in the position of triggering several contracts stored on its clients. Even if the oracle is honest, there is no guarantee of not having errors in its feeds. For this matter, Bertani proposes that oracles too must act as if they were miners, therefore their information go through a consensus mechanism. Ethereum's father Vitalik Buterin proposed in its white paper (Buterin, 2017) a decentralized data feed system where all the parties put in the system a given feed, for example the price spot of a commodity on a certain market, then the values falling between a certain percentile get a reward.

This idea was better explained by Vitalik on Ethereum's blog with regards to the concept of "Schelling points" or "focal points. In addition, Vitalik recognized the high possibility of a collusion attack, more or less a 50%+1 attack[19] (Buterin, SchellingCoin: A Minimal-Trust Universal Data Feed, 2017)[20].

[19] In my opinion this issue can be overcame introducing a bitcoin like consensus protocol in the way a feed is chosen and rewarded. Let's consider the limbo where transactions wait to be picked and insert in a block by a miner, instead of transactions we consider information (prices, rates, indicators and so forth). An "Oracle Miner" would build its own "Feeds' block" and then process it through the PoW, just as in bitcoin. Now things diverge from bitcoin because the block that has passed the PoW is not broadcasted clearly to the network but only its hash (of course in case of two or more identical hashes only the first one is considered valid). After a certain number of hashes has been "deposit" on the network the round is closed and no more ones are accepted. Now who was able to deposid a valid hash on time disclose to the network its feed's block. On the base of the data reported on different block several statistics are made (average and std for a stock's price, avg and std for bitcoin's price and so forth) the miner that was overall the closest to the maximum precision will be rewarded for that round, or all miners within a certain range of confidence on the base of their precision. I'm not able to confirm the validity of this idea so I'll let it open for anyone who wants to work on it.

[20] I wasn't able to find any reference but I think a decentralised data feed is possible. The idea is the same as the bitcoin protocol, the difference is miners would not collect transactions but information

Today there are several distributed ledger platforms, already working or on construction, and every one had to implement its own way to avoid Fig[22].


Distributed concurrence ●
Corda (R3 CEV) ●
Bitcoin
Colored Coins
Proprietary Metacoins
DAG (Directed Acyclic Graphs ●
Factom
Coinprism
PBFT (Practical Byzantine Fault Tolerance) ●
Derived PBFT (Hyperledger project) ●
RBFT (Redundant Byzantine Fault Tolerance, e.g., Evernym) ●
SBFT (Simplified Byzantine Fault Tolerance, e.g., Chain)
Casper ●
Ethereum (moving to PoS)
N2N
Proof-of-work
Proof of stake
PBFT and derivatives
Permissionless
Types of distributed mechanism
Permissioned
Openchain
PoET (Proof of Elapsed Time) by Intel (Sawtooth Lake Project) ●
Proprietary distributed ledger
Delegated proof of stake
Graphene ●
Steem ●
BitShares ●
Federated consensus
Round Robin
Leader-based consensus (including) PAXOS/ RAFT-based derivatives
Ripple (evolving into the inter-ledger protocol) ●
Stellar (Ripple fork)
MultiChain ●
Tendermint ●
BigChainDB ●
RAFT
Paxos (including many variances, such as Fast Paxos, Egalitarian Paxos, etc.)
Juno (Raft-Hardened Tangaroa; JP Project) ●
Tangaroa ●
Mencius
Viewstamped replication
ZAB

● **Denotes a consensus mechanism/distributed ledger technology evaluated as part of this paper. See Key Observations below.**
Note: Some DLTs provide for multiple consensus mechanisms, and these are configurable. A primary alignment has been established here for purposes of this paper.

Figure 22 Seibold Sigrid, an exhaustive view of different consensus protocols, KPMG.com

Marko Vukolic, taking as example Ethereum, stated that the current trend for blockchain is no more headed towards a being a simple mean of payment but to be a multi-purpose platform for a new generation of programs, smart contracts (see next paragraph), with many applications in any contexts[21]. For Vukolic this change of route makes blockchain. "step away from their original purpose and enter the domain of database-replication protocols step away from their original purpose and enter the domain of database-replication protocols, notably, the classical state-machine replication[22], and in particular its Byzantine fault-tolerant (BFT) variants." The main point is that a multi-purpose blockchain cannot implement a PoW

[21] I would say that the main reason Blockchain has become the buzzword is because of the huge possibilities of smart contracts.

[22] State-machine replication is a well-established approach to fault tolerance. The idea is to replicate a service on multiple servers so that it remains available despite the failure of one or more servers.

protocol because of its very high latency[23], as shown in Fig [23] which basically puts PoW and BTF to the antipodes of the graphic.

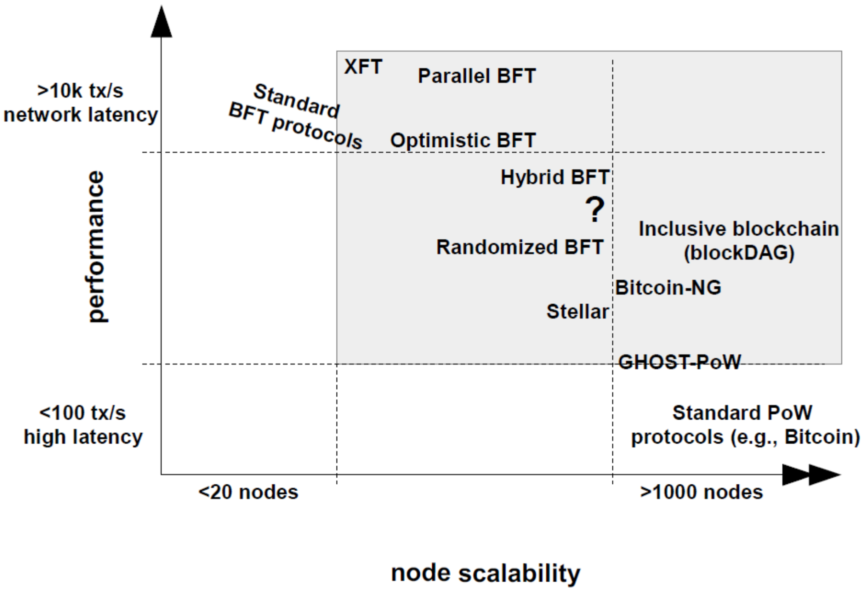
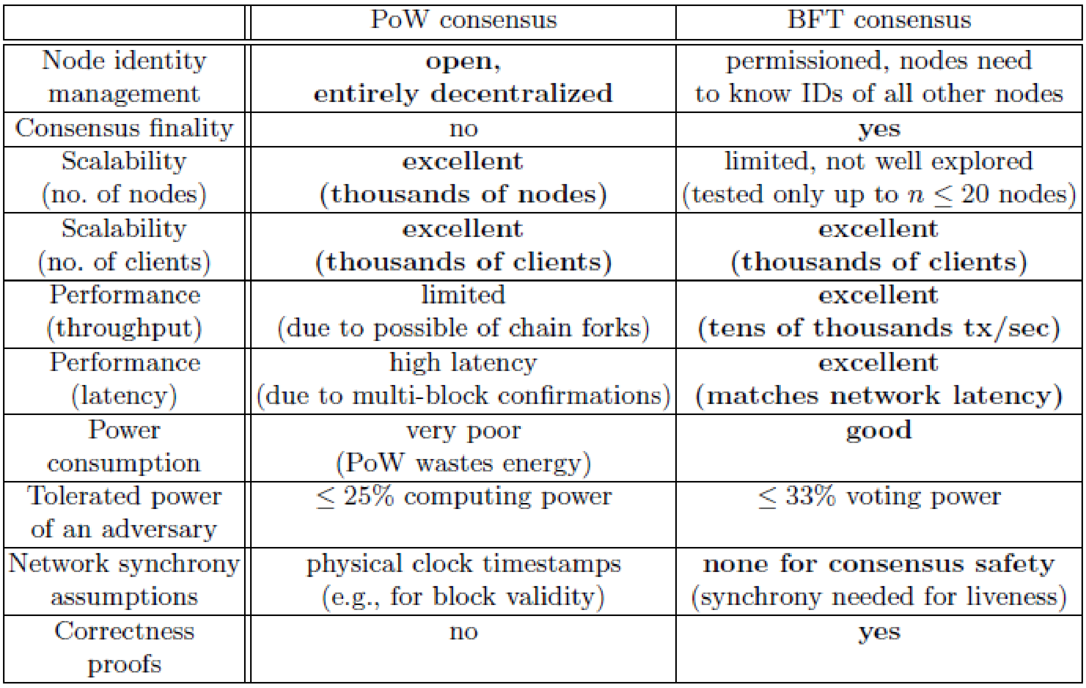


Figure 23 Trade off between network's size and its latency (Vukolic, 5/2016)

Fig[23] shows also that scalability of number of nodes using a BFT protocol is very poor compared to the traditional one. In the paper is reported that "having been invented in the context of replicating traditional applications, such as databases, for fault-tolerance, BFT protocols were never really tested thoroughly for their scalability beyond, say, n = 10 or n = 20 nodes" (Vukolic, 5/2016). The same paper provides also with a high level overview of how the two protocols deal in respect of different key performance indicators. Vukolic pointed as main difference the identity management system of the two. In PoW's blockchains, such as Bitcoin and Ethereum anybody can create its own node, download the blockchain or the source code, starting mining and so forth. The absence of gatekeepers or intermediaries allows also the preservation of the actual identity of whoever control a node. In contrast, BTF's systems require all node to disclose its identity. That would require a central authority to act as the gatekeeper, hence going against what Bitcoin was

[23] Increase the scale of a system increase as well it's latency, the time the input is sent and the output is delivered

born for. Still it is easily predictable how such thing would have been required nevertheless by a controlling authority[24].



	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all other nodes
Consensus finality	no	**yes**
Scalability (no. of nodes)	**excellent (thousands of nodes)**	limited, not well explored (tested only up to $n \leq 20$ nodes)
Scalability (no. of clients)	**excellent (thousands of clients)**	**excellent (thousands of clients)**
Performance (throughput)	limited (due to possible of chain forks)	**excellent (tens of thousands tx/sec)**
Performance (latency)	high latency (due to multi-block confirmations)	**excellent (matches network latency)**
Power consumption	very poor (PoW wastes energy)	**good**
Tolerated power of an adversary	$\leq 25\%$ computing power	$\leq 33\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	**none for consensus safety** (synchrony needed for liveness)
Correctness proofs	no	**yes**

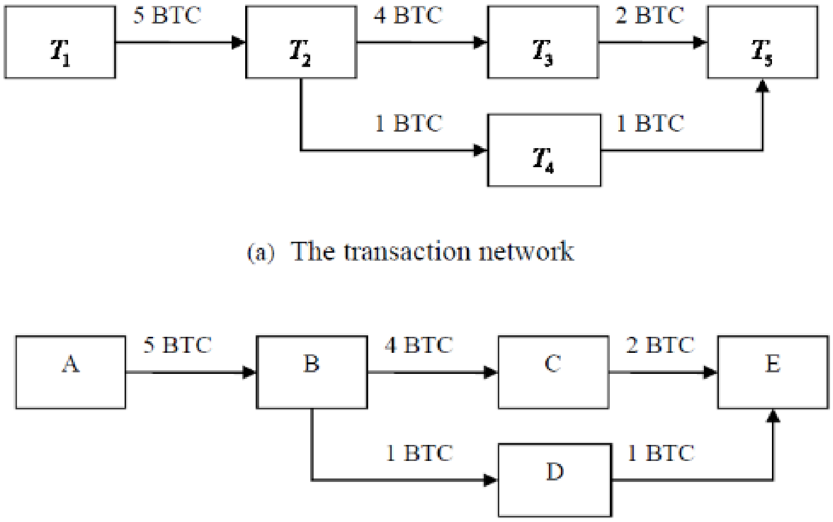
Table 4 High-level comparison between PoW and BFT blockchain (Vukolic, 5/2016)

1.2.6 Anonymity

Anonymity is a key and fundamental aspect of Bitcoin, but not necessarily for every distributed ledger platform. In Bitcoin every user is identified by his public keys and, in order to get a private key, no information about the person or the organization are asked and no information can be obtained by the sole address. Despite this "static" anonymity Bitcoin protects his users with a pseudo-anonymity, indeed on a distributed ledger, where all the historical of transactions are recorded for ever, it is possible to construct a map and identify the identities using the structure of transactions and users networks Fig[24], that are respectively the flow of bitcoins between different transactions, each vertex represent a transaction while each edge is the output between a source and a target, and the flow of Bitcoins

[24] About what regulators might or might not allow there is going to be a full chapter ahead in this review.

between users, which are the vertex while the edges are the transactions. (Reid & Harrigan, 5/2012) (QingChun & Yu, 10/2015)



(a) The transaction network

Figure 24 QingChun ShenTu, Transaction and user network, Research on Anonymization and De-anonymization in the Bitcoin System

To achieve a user identity, alongside the two networks, there is the need of information gathered off-network. In their work (Reid & Harrigan, 5/2012) argue that many businesses which accepts Bitcoins as payments have records of their clients, this records may be sent for by some authority, hence unveiling the owner of a certain public key and then starting the analysis of the network from that point. In the same work, it has been reported of several approaches to analyse the network.

The de-anonymization of a blockchain identity has been felt by the academic as a very urgent issue indeed the production and proposal of solutions, depending on the type of method used to break into it, has resulted as one of the most prolific. (Vasek & al, 10/2014), (Heilman & al, 8/2016). However, if compared to traditional virtual payments system such as Visa, Bitcoin offers a level of anonymity of a whole different level, comparable to cash exchange, as stated in the introduction of Handbook of Digital Currency at page 18 (Chuen, 2015).

There are several attempts to provide users with full anonymity while operating on distributed ledgers. An article from bitcoin.com presents the top three full anonymity cryptocurrencies now available (Redman, Meet the Top 3 Coins in the Cryptocurrency Anonymity Race, 2017):

- Zcash is a “decentralized and open source cryptocurrency that aims to set a new standard for privacy and anonymity through the use of ground breaking cryptography”. Zcash is actually a fork of Bitcoin which preserves transactions using the “zero proof” protocols which allows a node to be sure that another node has knowledge of a certain piece of information without any need to disclose it entirely or just partially (Quisquater & all, 1989).
- Dash (a.k.a. Darkcoin) implements the “DarkSend” technology, which merges transactions into anonymous bigger ones, and then a randomly selected node is elected as a master one to create the transaction in a decentralized way. The master node for a certain round is in charge to determine which transaction can be allowed into the pool. Finally, Dash implements a PoW based upon the X11 hashing instead of SHA256 (Duffield & Hagan, 2017).
- Monero is not a clone of Bitcoin since it was derived from another alt-coin named as Bytecoin[25]. Monero is distributed decentralized through a PoW but its transactions are signed through a “ring signature” which has been described as “digital signature that specifies a group of possible signers such that the verifier can’t tell which member actually produced the signature” (Rivest & al, 2001). In addition, Monero is capable to hide the amount transact and also the destination of it, hence enhancing the privacy of a user (Noether, 2015).

[25] Such a remarkable originality

1.2.7 Smart contracts

“The code is the law” is a motto[26] that states that on a blockchain everything must proceed according to what it has been written in its code without any other kind of external intervention. This concept is a consequence of the “immutability” of a blockchain.

Starting from this assumption, which can also be not true if we consider Ethereum and its hard fork after the DAO issue[27], “Smart contracts combine protocols, users ’ interfaces, and promises expressed via those interfaces, to formalize and secure relationships over public networks. This gives us new ways to formalize the digital relationships, which are far more functional than their inanimate paper-based ancestors. Smart contracts reduce mental and computational transaction costs, imposed by either principals, third parties, or their tools” (Szabo, 09/1997). In his paper, Szabo reported that smart contract could overcome transaction costs if their design is observable, verifiable and private. The first objective called observability means that all the counterparties of the contract are able to observe how they are behaving with respect of that particular contract; lack of observability may allow moral hazard and other opportunistic actions. The second objective of a well designed Smart contract is the presence of an adjudicator capable of identify the presence of a breach in the contract, Szabo suggested that this possible only if the contract is highly verifiable. The third and final objective is the privacy of the contract, meaning that its prerogatives are known only among the parties involved in it. This emphasises how the contract is managed only by its code and no by third parties, therefore also the adjudicator should be embedded in the code (Hillbom & Tillstrom, 02/2016).

[26] Perhaps taken from the third movie of “Pirates of the Caribbean” (www.youtube.com/watch?v=Y6OvsJqimfg)

[27] http://ethereum.stackexchange.com/questions/6335/if-ethereum-does-a-hard-fork-to-return-exploited-funds-from-thedao-does-this-ca

In an article published on CoinDesk Josh Stark, head of operations and legal at Ledger Labs, declares there is a great deal of confusion around smart contracts and their definition: “They are defined variously as “autonomous machines”, “contracts between parties stored on a blockchain” or “any computation that takes place on a blockchain” (Stark, 2017). In this article it has been noted how different definitions still tend to fall within a pair of categories:

- Smart contracts as “Smart contract code”, the program itself is recorded on the distributed ledger, which gives to it the properties of permanence and resistance to censorship, the program can itself control the ownership of the underlying assets and it is executed by the distributed system, meaning that it will be always triggered as it was uploaded in the first place.

  In many applications, “smart contract code” is not used singularly but in concert with others as small pieces of larger and more complex usages, for instance the DAO on the Ethereum blockchain.

  A valid critique towards these definitions is they do not really catch the broader field of usability of these contracts. They fails to capture their “independent agency” property.

  For this reason some authorities prefer referring to them as “smart Agents”, analogous to the concept of software agents
- Smart contracts as “Smart Legal Contracts” refer to their usability as a complement or even a replacement to existing legal contracts. For intuitive reasons these software should be written with a language capable to express legal concept in a way understandable by computers. This category of definitions has been applied to contracts stored on Corda blockchain.

  From this aspect many argues simply translate legal contract into code may be a use not efficient of the potential that distributed ledger technologies has. Therefore, Stark pushes towards a revolution in how contracts are written and enforced.

From this two categories Christopher Clark of the UCL and Vikram Bakshi from Barclays (Clack & Bakshi, 08/2016) proposed an unifying definition: “A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution".

In a subsequent work, Clark and Bakshi developed the template of a smart contract from the framework of "Ricardian Contracts[28]" triple of "prose, parameters and code", of Ian Grigg (Clack & Bakshi, 12/2016). In this study, they provided with the essential requirements of a smart legal contract:

- Methods to create and edit smart legal agreements, including legal prose and parameters.
- Standard formats for storage, retrieval and transmission of smart legal agreements.
- Protocols for legally executing smart legal agreements (with or without signatures).
- Methods to bind a smart legal agreement and its corresponding smart contract code to create a legally enforceable smart contract.
- Methods to make smart legal agreements available in forms acceptable according to laws and regulations in the appropriate jurisdiction.

Currently there are several projects developed to implement different kinds of smart contracts on the Bitcoin's blockchain, these project are labelled as "coloured coins". Several other proposals seek the design and implementation of these contracts on different blockchains such as Ethereum and Hyperledger[29].

[28] "A Ricardian Contract can be defined as a single document that is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carries the keys and server information, and g) allied with a unique and secure identifier (Grigg, 2017).
It is a method to describe "value" in financial cryptography. An unique and unforgeable identifier is obtained with the already mentioned hashing functions.

[29] Ethereum is going to be presented extensively in the next chapter about DL platforms

1.2.7.1 Coloured Coins

The “colored coin” project aims to expand the properties of bitcoin to other assets through the implementation of smart contract directly to the bitcoins’ Blockchain.

“While originally designed to be a currency, Bitcoin supports a limited scripting language that can be used to store metadata on the blockchain. Coloured Coins is a concept that allows attaching metadata to Bitcoin transactions and leveraging the Bitcoin infrastructure for issuing and trading immutable digital assets that can represent real world value. The value of such digital assets is tied to a real-world promise by the asset issuers that they are willing to redeem those digital tokens for something of value in the real world.

Digital assets on top of the Bitcoin Blockchain can be used to issue Financial assets (securities like shares, commodities like Gold or new currencies), prove ownership (A digital key to a house or a car, a concert ticket), store information (Documents, Certificates) or create smart contracts.

The advantage given by using the blockchain as the backbone for such asset manipulation is that one can rely on the blockchain’s transparency, immutability, ease of transfer and non counterfeitability to transfer and trade such digital tokens with unprecedented security and ease.” (Leiba, 2016)

Smart Properties has been proposed as a possible usage for colored coins, this contract uses the last ownership transaction as an input in a new transaction. The ownership then is represented with the public key hash. (Hillbom & Tillstrom, 02/2016). Smart ownership then may be declined in several scopes like land administration register for “the process of determining, recording and disseminating information about rights, value and use of land” (Anand & al, 03/2016); Smart financial assets (Van de Velde & al, 2016).

1.2.8 Distributed Technologies Ledger platforms

1.2.8.1 Bitcoin

Bitcoin is an online peer-to-peer payment system with its own currency, completely virtual, not like fiat[30] money that you may have in your pocket or on your bank account. Bitcoin, of course, it is used as a mean to transfer value from an entity to another through a transaction, like every other currency, and everything is done thanks to the its blockchain. Fig.[25] shows in an elementary way how the Bitcoin's blockchain works.

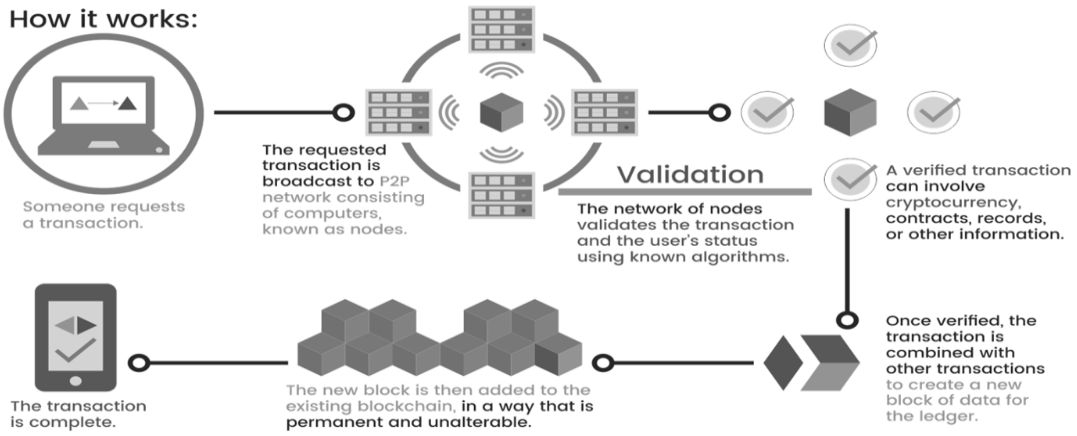

How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Figure 25 How a Blockchain Works

Bitcoin uses the Proof of Work[31] protocol to reach consensus among its nodes. Consensus for this matter is reached when all the non faulty members of the platforms agree to update their copy of the ledger to the same version, hence accepting all the changes or the transactions suggested by other members. This protocol is enforced at every round, about every 10 minutes, by special nodes named "miners" that compete among themselves to be first into enforcing it, hence receiving a reward in newly minted bitcoins plus transaction fees.

[30] Something, also a piece of paper, established as money from a central authority (fiat from Latin "let it become")

[31] Since this work is supposed not to be seen just by computer scientists, on the contrary of many research paper I've gone through, I decided to explain the following topic in a detailed manner but still assuming a novice friendly approach.

In the Bitcoin network a transaction is immediately broadcast to the transaction pool, that is the "limbo" of not yet verified transactions. Miners pick up transactions[32], more than 5000 per block (Antonopoulos, 11/2015), and then they start to verify if there are non-legit ones. I.e. a transaction that is higher than the sender current account, a transaction without a correct owner's pubic key or illegal contents in the transaction.

Miners would be more incentivized to embed into a block as much transactions as possible in order to collect higher fees; Bitcoin does not allow this kind of behavior because on its blockchain there is a size limit of one Mb per block.

The Bitcoin's protocol has been developed in order to allow an average[33] of six blocks creation and roughly, 25.200 transactions per hour, by comparison Visa today processes on average 7.200.000 transactions per hour and has been built to manage up to 201.600.000. Scalability of Bitcoin, its ability to keep up with its own success and therefore increase of users is a major issue, which is dividing the community about how to address it *(Croman & al, On Scaling Decentralized Blockchains, 2/2016)*. By the time I am writing there are at least two proposals to overcome the problem of scalability:

- Increase the block's size through a hard fork. Shifting the limit on higher levels would allow more transactions per second and miners would be less demanding in terms of fees to insert a transaction in their blocks. The opposition to this course of action argue that hard forks take time to raise sufficient consensus, full nodes would be required with larger storage space, therefore hurting decentralisation[34] (Phantomcircuit, 2016). On a proposal paper, submitted for the "Financial Cryptography and Data Security 2016" conference, it has been stated maximum size of block must not exceed four

[32] Usually a transaction to be picked by a miner should be comprise of a fee for it, otherwise it will be ignored for others with higher fees.

[33] The fact that is an average is the consequence of very important concept detailed ahead

[34] Less people willing to download the whole blockchain setting a full node, which are the backbones of Bitcoin's protocol.

Mb and latency limit cannot be lower than 12 seconds (Croman & al, On Scaling Decentralized Blockchains, 2016).

- Segregate Witness (Segwit) and lightning network. It has been proposed during Scaling Bitcoin 2015 held in Honk Hong by Dr. Piter Wuille[35]. The logic behind Segwit is that full nodes are, for the most part, not mining nodes, hence most of the information stored on the blockchain are not necessary. Signatures are absolutely necessary for validating transactions, which is done by miners which are of course full nodes but not all full nodes are miners. The benefit coming from removing signatures from one Mb blocks is the size of those could be increased. Therefore, more transactions can be included into newly mined blocks increasing the volume per second. I would like to make the reader understand that, even if it could seem somehow that signatures are just a minority part of the size of a block, it is a huge save of space. Wullie stated that if a block were composed just by Segwit transactions the actual number of them into a 1Mb block would be equal to a block increase of four times, for blocks without Segwit (van Wirdum, 2016). Finally one another, allegedly, argument in favour of Segwit is that it does not break any consensus rule; hence, its implementation would be considered a “soft fork”[36]. Lightning is another solution to scalability proposed by Poon and Dryja (Poon & Dryja, 2016). The idea is to implement a network of micropayments channels. Two nodes can agree, mathematically through a smart contract stored on the blockchain, to create a channel were exchanging Bitcoin among themselves for a period without having to broadcast every transaction to the network but only, at a certain date, the final position of the two party. This would be fully secure because of the hash[37] proof of existence of a certain transaction. This solution can lead to a huge number of possible applications among self-

[35] https://www.youtube.com/watch?v=NOYNZB5BCHM

[36] When a blockchain does an hard fork it means that different fork transactions can’t be processed into the same block, because there has been implemented a different set of consensus rules. On the contrary transactions that come from different directions of a soft fork have the same set of rules therefore they can be processed into the same block.

[37] Hashes functions will be introduced few pages ahead.

trusting parties, for example two business units of the same company, as well as cash flows from a supplier to a client. Therefore, lightning can enable countless transactions off-chain that, eventually, will demand the same amount of work to be embedded on the blockchain as a single one.

- Blockstram, one of the most influent company involved in the Bitcoin and blockchain industry, presented as a potential solution the implementation of sidechains. Sidechains are complementary ledgers pegged to the main one, usually Bitcoin. Assets can move back and forward from a chain to another by escrowing them one the departing chain, freezing them in other terms, while creating their proxies on the other one Fig. [26]. In this way it can be possible to create blockchains with different features, for instance grater block sizes, higher block's generation frequencies, different assets and so forth without losing contacts with the main one (Back & al, 2014).

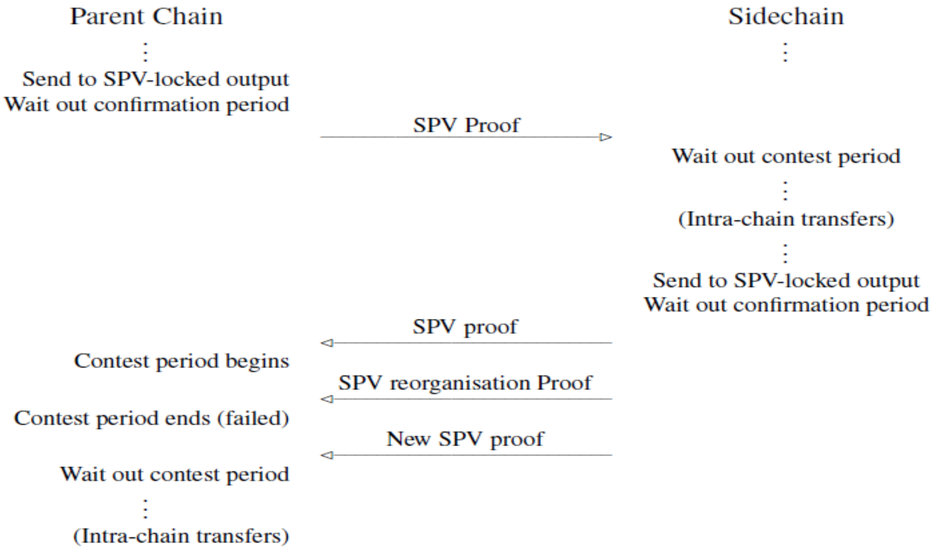


Figure 26 Example two-way peg protocol (Back & al, 2014)

After the verification of the legitimacy of the transactions, the miner starts its Proof of Work. The aim of this task is to make miners wasting energy and hardware in order to raise the requirements needed to launch an attack to the blockchain like a Sybil attack, that is subverting the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a

disproportionately large influence (Alchemi, 2016). In the scenario of a Sybil attack, an honest node may be unable to connect to non puppet nodes, de facto disconnected from the network and vulnerable to double-spending attacks[38]. Nakamoto refers to the blockchain without the Proof of work as a system where consensus is based on a majoritarian protocol with "one-IP-address-one-vote", now the system runs with "one-CPU-one-vote"[39].
Proof of work was actually not intended for consensus application on the first place. Proof of work was devised as a shield against junk emails and spamming by increasing the unitary cost to delivery an email through the implementation of pricing functions (Dwork & Naor, 08/1992). The proof of work aims to obtain an output of a pricing function complaint with certain arbitrary conditions[40].

Sending one million emails it is a task not very complicate therefore not very expensive, for even cheap hardware. The idea is to impose to the sender the solution of a pricing function f :

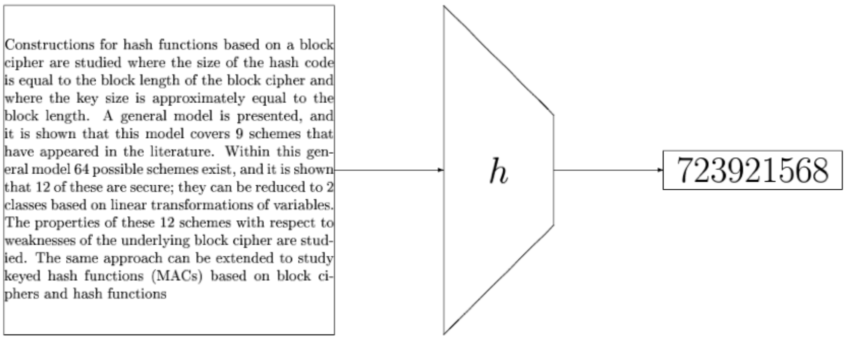
- f is moderately easy to compute, this condition must be fixed during time, therefore advances in hardware and solution algorithms must be taken into consideration
- f is not amenable to amortization, so there is a significant difference in computer resources, time and energy, between computing f one time and computing it millions of times
- Given x and y it is easy to determine if y=f(x), that means the function is asymmetrically expensive; the receiver must not spend the same resources of the sender.

[38] Since, from that moment on, all the blocks the honest node would receive will be created by the malicious part, which has no intention to notify the transactions to the real network. In this way as long as the hones node is trapped it will take as legit all the coins received from the attacker and, when the fraud comes to an end and it is again reconnected to the network, lose them all as soon as it re-upload its copy of the blockhain.

[39] The deeper meaning of this statement will be more clear after the explanation of the Bitcoin's protocol

[40] For example Bitcoin accept only outputs with a certain amount of zeros before the rest of the output, this requirement will be clearer as soon as the concept of nonce will be introduced.

There are a certain number of these functions suggested in the work of Work and Naor, but for this chapter the focus has been placed upon Hash Functions for cryptographic purposes. Hash functions are mathematical algorithms that maps binary strings of arbitrary length to binary strings of a fixed length, like 64 or 128 bits Fig[27]



Constructions for hash functions based on a block cipher are studied where the size of the hash code is equal to the block length of the block cipher and where the key size is approximately equal to the block length. A general model is presented, and it is shown that this model covers 9 schemes that have appeared in the literature. Within this general model 64 possible schemes exist, and it is shown that 12 of these are secure; they can be reduced to 2 classes based on linear transformations of variables. The properties of these 12 schemes with respect to weaknesses of the underlying block cipher are studied. The same approach can be extended to study keyed hash functions (MACs) based on block ciphers and hash functions

Figure 27 Schematic exempla of an arbitrarily long string processed with a generic Hash function (Patel, 2008)

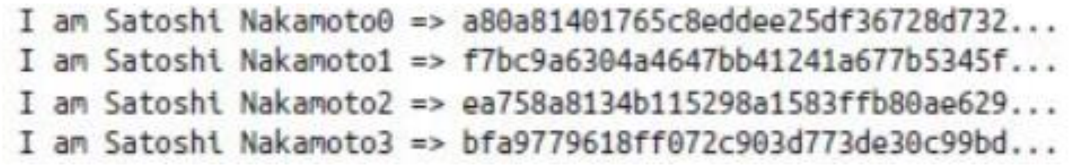
An Hash function to be an useful instruments increasing the costs of spamming must be a one way operation, hence “Given only a digest, it should be computationally infeasible to find a piece of data that produces the digest (pre-image resistant)” (Patel, 2008).

There are many Hash functions but, likewise to pricing functions, I am going to take into account just the sub set known as “Secure Hash Algorithm” or SHA[41], since it has been used for Bitcoin. It is a one way function, from any input I can always find its hash but do the reverse it could takes an indefinite amount of time, since a brute force approach would be the sole way.

Bitcoin uses a hashing function based on the Secure Hash Algorithm 256bit (SHA256) (Nakamoto, 2009). SHA256 is part of the group known as SHA-2 that

[41] The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), including: SHA-0, SHA-1, SHA-2 and SHA-3.

has the particularity to be collision resistant[42] (Amy & al, 2016) an example in Fig. [28].



```
I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
```

Figure 28 Exempla of a Hash256 transformation (Chan, 2016)

From the example, we can see that the string "I am …." processed with SHA256 gives completely different hashes by just changing one/two digits.

At this point, we have the proper pricing function, now we need its digest. The input for the PoW in Bitcoin is the "Block Header" that is an 80 bytes, a file that contains several information Tab. [5].

Size	Field	Description
4 bytes	Version	The version of the software's protocol
32 bytes	Previous Block Hash	The reference to the parent block in the chain
32 bytes	Merkle Root	The hash of the root of the Merkle tree
4 bytes	Time Stamp	The approximate creation time of that block
4 bytes	Difficulty Target	The PoW difficulty target for this block
4 bytes	Nonce[43]	The solution to the Proof of Work

Table 5 The structure of the block header (Antonopoulos, 11/2015)

In the Bitcoin protocol the block header is created by the miner, it goes through a double cycle of SHA-256[44] and the output is the Block's hash. In order to be attached to the blockchain the Block's hash must meet the protocol's conditions. For the Bitcoin blockchain the condition is the candidate block's hash must start with a number of zeroes even or higher to the target's difficulty[45].

[42] Resistance to collision means it is computationally infeasible to find two different strings that generate the same Hash, using the same Hash function.

[43] in a bitcoin block is a 32-bit (4-byte) field whose value is set so that the hash of the block will contain a run of leading zeros

[44] Block header → SHA-256 → h' → SHA-256 → h''

[45] Difficulty is a measure of how difficult it is to find a hash below a given target.

The Header is a lighter file if compared to the average overall block's size, 80 bytes against 1 Mb, but it has been devised to be able to store all the information needed for nodes that are not provided with the entire blockchain, what we introduced it the node subchapter as "lightweight" nodes[46]. These nodes run what Nakamoto labelled as "Simplified Payment Verification"[47].

The difficulty is the number of initial positions in the block's hash. It is trivial to understand that as higher the difficulty the higher is the number of zeroes. "To give a simple analogy, imagine a game where players throw a pair of dice repeatedly trying to throw less than a specified target. In the first round, the target is 12. Unless you throw double six, you win. In the next round, the target is 11. Players must throw

10 or less to win, again an easy task. Let us say a few rounds later the target is down to five.

Now, more than half the dice throws will add up to more than 5 and therefore be invalid. It takes exponentially more dice throws to win, the lower the target gets. Eventually, when the target is 2 (the minimum possible), only one throw out of every 36, or 2% of them, will produce a winning result" (Antonopoulos, 11/2015).

The Bitcoin protocol calculate the number of seconds it took to add 2.016 new blocks to the chain, if this value is lower than 1.209.000 seconds (two weeks) the protocol increases the difficulty of the challenge to maintain the 10 minutes per block average. The protocol uses the timestamps; the moment the block was chained, stored in each block to calculate whether or not to increase the difficulty.

Anyone can go on http://blockchain.info and see Bitcoin's blockchain by itself, the current block has a hash of 18 zeros. Nakamoto devised this dynamic in order to offset technological advancing of CPUs, therefore maintaining as long as possible fixed the 10 minutes time frame.

The Proof of work is double-hashing billions of times the block header, changing the nonce, until a miner finds a block's hash that complains with the current

[47] It will be fully explained with the introduction of the Merkle tree root concept

difficulty. The first miner to achieve the task broadcast the block and the solution to the whole network, which will verify the legitimacy of the claim and will attach the block to the blockchain. After that a new round of mining will immediately start. The nonce is of paramount importance for the mining process, is the variable miners make change countless times per second in order to generate as much different block hashes as possible[48]. Because of the non collision property of SHA-256 a nonce is unique therefore, it cannot be used more than once preventing an easy forging of fraudulent blockchains.

A human being, under the assumption that it acts with the final aim of obtaining a profit, would never waste time, money and valuable resources just to ensure that the transactions of others are legit. This person, if in possession of enough computing power, would more likely try to overrun the network with a 51% attack[49]. The minting system of Bitcoin, and last piece of this consensus protocol, prevents this eventuality by rewarding the miner every time it is able to add a new block. , at the beginning the reward was 50 Bitcoins per block chained, the 28th of November 2012 it was automatically halved to 25, the 9th of July 2016 it was cut in half a second time while the next reduction is set the 4th of July 2020 (Bitcoinblockhalf.com, 2016).

Forcing miners to solve puzzles in order to add to the ledger provides protection: to double-spend a bitcoin, digital bank-robbers would need to rewrite the blockchain, and to do that they would have to control more than half of the network's puzzle-solving capacity. Such a 51% attack would be prohibitively expensive: bitcoin miners now have an aggregate power of 1.68 ExaHash, this is more than 43 thousand times the hash power of the top 500 supercomputers in the world combined (O'Ham, 2012).

[48] Since the all the components of a Block header are fixed, version, previous block's hash, the Merkle root, and the difficulty (time of course is not fixed but its precision is limited to the seconds therefore, considering that some miners hash in the order of the thousands of billions iterations per second it is like a fixed variable)

[49] If a single node possess more than the 50% of the hashing power of the network then it will be able to forge a blockhain faster than the honest nodes, this would enable the possibility for it to do double spending by transact coins on the legit blockchain and over write it distributing its forged copy of the blockchain where that transaction is not accounted.

The drawback in the figures I have just presented is the energy consumption the Bitcoin's system requires. The problem was highlighted in 2014 by O'Dwyer and Malone (O'Dwyer & Malone, 2014) who stated that PoW had required as much electricity as the whole Ireland, the 29th of march the magazine "Motherboard" took on again the topic predicting that in 2020 the energy wasted would have risen to 14 Gigawatts, the equivalent of Denmark's power generation, with an average of 5,5 kWh per Bitcoin mined, more or less as much as the annual American household consumption (Deetman, 2012).

The consensus protocol the author descripted from the paper of Nakamoto, with the aid of "Mastering Bitcoin" of Antonopoulos, has been analyzed through several papers

The Merkle tree root is an instrument to save storing space on a node loaded upon devices with very limited storage capacity. It has been explained how a string processed through an hash function will always return the same hash, of course with the trivial condition that no modifications are made on the string nor the hash operator. This property makes pointless to store on lightweight nodes all the transactions ever made since the "creation block"[50] in order to check the validity of payments.

Fig. [29] shows a Merkle tree created from four different data blocks, which in our case are four different transactions. Hashing firstly the single transactions and then reiterating over and over a single hash is obtained, this hash is called the root it is unique and it proves that no modification has been done in the block[51].

[50] The term to indicate the first group of transactions ever mined

[51] This verification is very efficient since it takes at most 2*log2(N) calculations, with N the number of Data elements (Antonopoulos, 11/2015)

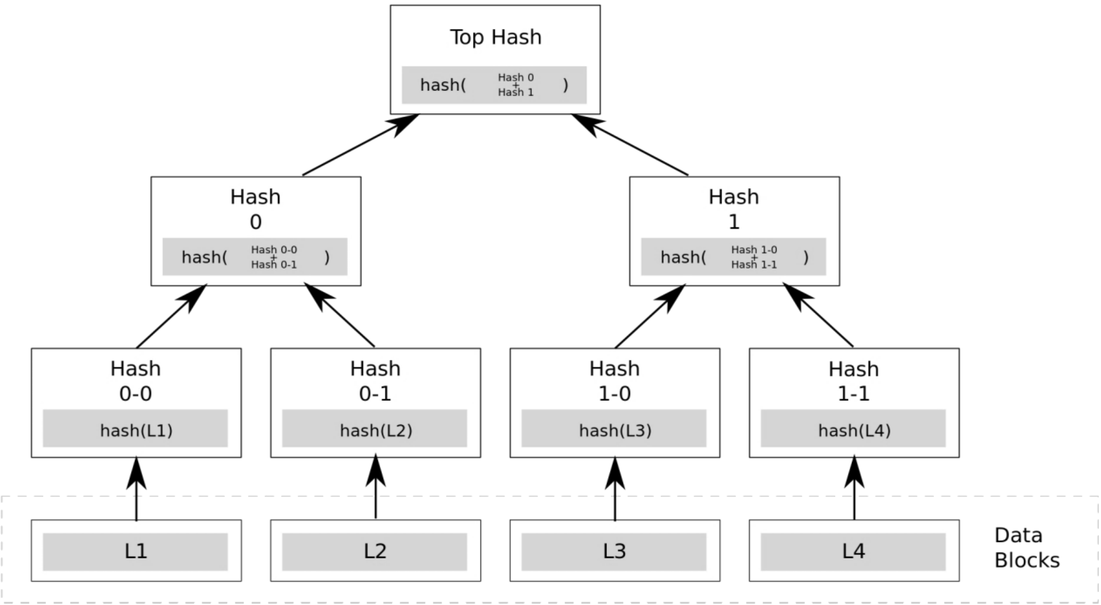


Figure 29 Merkle tree from four initial data blocks (contributors, Merkle tree, 2016)

Having gone through, at least, the most important components of Bitcoin's consensus protocol allows to list the most relevant consequences of it.

- Bitcoin has successfully decentralized consensus because it has worked as a payment system for more than 6 years, so far, without the necessity of a trusted central party. This achievement is commonly referred as trustless consensus (Silverberg, 2016) because the validity of the ledger is stricuy defined by unsubvertible mathematical unsubvertible parameters.
- Transactions on the Bitcoin network are not reversible. As soon as a transaction gets insert in a mined block they are like "carved in the stone", therefore there is no mean to undo them. For example if the address of the contains a mistake the payment will go to another node, in a situation like this normally it would be possible to contact the bank deleting the wrong payment, on a blockchain like Bitcoin this is not possible and the coins are lost for ever (Ateniese & al, 2016). In the following chapters about the possible implementations of distributed ledgers, not only blockchains, it would be presented several pro to the immutability property.

Bitcoin is a peer to peer system, anyone can join it creating its own "identity" by generating its private key without having to disclose any personal information

1.2.8.2 Ethereum

Ethereum is an unpermissioned DLT platform for applications, it is the second biggest[52] blockchain on the market (Unknown, Crypto-Currency Market Capitalizations, 2016), created by Vitalik Buterin and Gavin Wood (Wood, 2016) (Buterin, White Paper: A next generation smart contract & decentralized application platform, 2012). "Ethereum, taken as a whole, can be viewed as a transaction-based state machine" in the sense that, in contrast with Bitcoin, it doesn't use transaction inputs and outputs "In bitcoin's model, each newly minted bitcoin becomes an unspent transaction output with an owner who retains the right to consume that bitcoin at a later time. During a bitcoin transaction, these "unspent transactions outputs" become the inputs that are "consumed" in the transaction. When these bitcoins are spent, or pushed, to another user, a brand new UTO is created" (Dienelt & Rizzo, 2016). Ethereum uses a different method that saves the most recent "state" of its Blockchain, the list of accounts and their own balances and a transaction, to be valid, relies on the sufficiency of balance of the sender.

Ethereum currently works with a consensus protocol based on proof of work with the pricing function EthHash, it has been planned to move to the proof of stake protocol in the future, and like Bitcoin, it has its own currency the "Ether". Like Bitcoin, new Ethers are minted every time a new block is added to the blockchain. Unlike Bitcoin there is no limit to the number of Ethers and no progressive decreasing system. Every 12 seconds five new Ethers are minted.

Ethereum plans to adopt in the future a Proof of Stake (PoS) (Anderson & al, 6/2016) a system that replaces the concept of "one CPU one vote" with "one token one vote" or rather than consuming some physical resource, perhaps miners should consume the cryptocurrency itself, thus "bootstrapping" the security of the system from its own value, rather than requiring expensive and energy-intensive mining

[52] By market cap value of its tokens

operations. (Poelstra, 3/2015). PoS has not yet being accepted by the community as a suitable replacement for PoW, the argument against its implementations are connected to its incapability to waste valuable resource in the process and, by extension, produce randomness through entropy generation, which is essential in cryptography (Lenstra & Wesolowski, 5/2016) (Poelstra, 3/2015). To replicate the waste of scarce resources of a PoW it has been proposed to destroy actual coins, that has been called Proof of Burn (PoB), and the probability of winning the reward from mining the block would have been the ratio of how many coins the miner sacrificed and the total amount burned in that round. This may be implemented alongside with a less energy demanding PoW to avoid some of the issues highlighted before with the PoS (Stewart, 5/2014)[53].

In the article of Alexander Chepurnoy, not yet peer reviewed, there are several example of possible weaknesses of a PoS, such as "Grinding Attacks", going reverse into the blockchain history with a small amount of tokens and subvert a past block and do that repeatedly until the malicious miner has taken over the blockchain. "Private forks and nothing at stake attacks" imply that, since there is no waste of resources, for every node is as much as convenient to vote for a sole fork or for N forks. Attackers may just spend its coins from one of the many forks and then ignore it by voting, in the future, just for the remaining N-1 ones (Chepurnoy, 1/2016).

Ethereum's blockchain belongs to the permissionless denomination of distributed ledger platform, like Bitcoin anyone is able to work on it design their script in high-level languages, such as Javascript for example, and then store them on the blockchain that are compiled into the native language of Ethereum, Ethereum Virtual Machine Byte Code[54] (Luu & all, 10/2016). The Ethereum Virtual Machine is part of the Ethereum's protocol, it allows anyone to execute its code on the blockchain.

[53] Proof of burn has just be proposed, not implemented.

[54] A low level, stack-based bytecode language

While Bitcoin has blocks of a predetermined size of one Mb Ethereum has not such limit, because it would prevent from the possibility of implementing "Turing Complete[55]" contracts. Ethereum implement a disincentive known as "Gas" that prices in real time how much a contract costs to be stored on the blockchain. In this way, a memory saving contract design is desirable in order not to pay too much for creating it. Fig30[] shows the state transition of states during a transaction on Ethereum, which starts when a transaction is well formed, otherwise it would generate an Error message; also if a contract is involved then the "Gas" system is set in function. If ether and/or Gas are insufficient, the states are reverted to their initial form apart from the fees, which are the payment to the miner that processed that transaction and that would have incorporated it into a block.

Ethereum ultimate goal is to host a large number of smart contracts which communicate one with another creating what they call a Decentralized Autonomous Agent (DAA) or a Decentralized Autonomous Organization (DAO) (Buterin, DAOs, DACs, DAs and More: An Incomplete Terminology Guide, 2016).

[55] Turing completeness, named after Alan Turing, is significant in that every plausible design for a computing device so far advanced can be emulated by a universal Turing machine — an observation that has become known as the Church-Turing thesis. Thus, a machine that can act as a universal Turing machine can, in principle, perform any calculation that any other programmable computer is capable of. However, this has nothing to do with the effort required to write a program for the machine, the time it may take for the machine to perform the calculation, or any abilities the machine may possess that are unrelated to computation. While truly Turing-complete machines are very likely physically impossible, as they require unlimited storage, Turing completeness is often loosely attributed to physical machines or programming languages that would be universal if they had unlimited storage. All modern computers are Turing-complete in this sense. (Unknown, 2016)

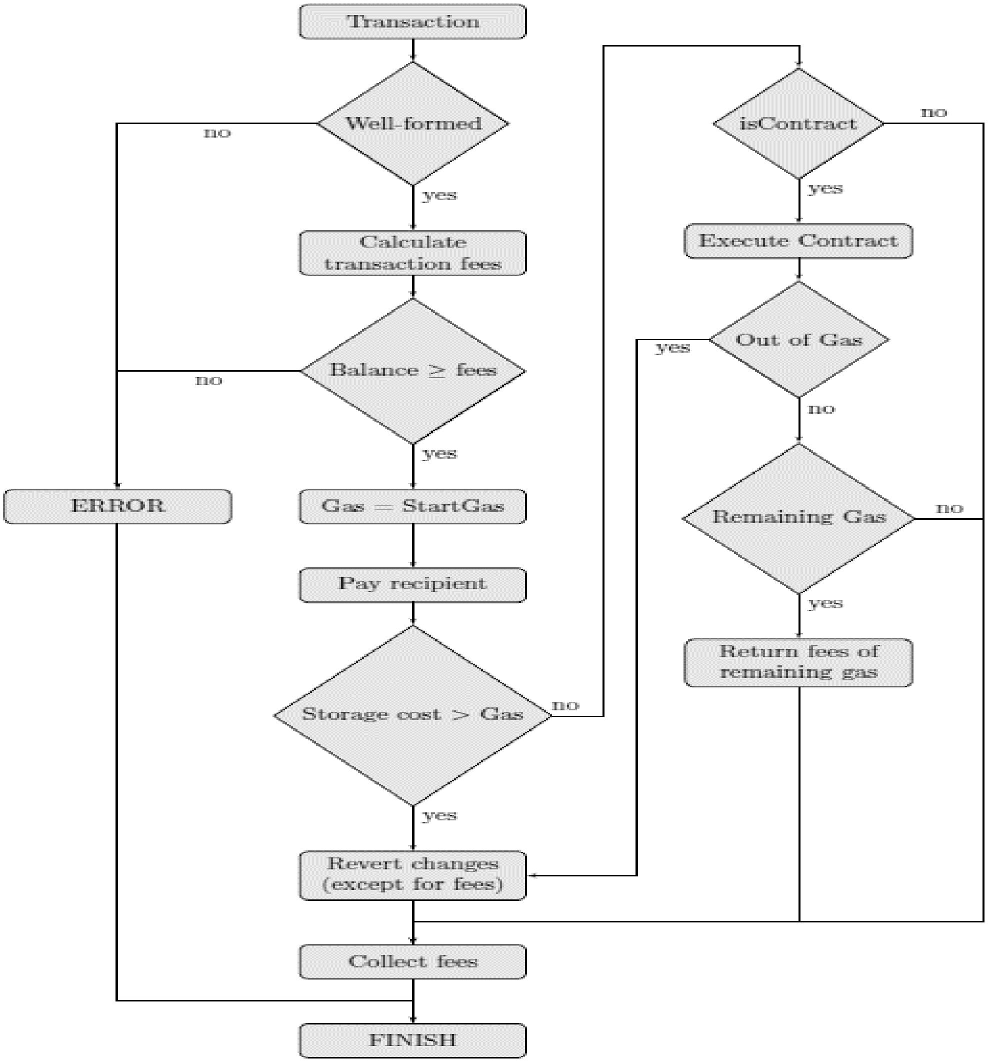


Figure 30 Flowchart visualising the Ethereum state transition function (Hillbom & Tillstrom, 02/2016)

1.2.8.3 Fabric

Hyperledger is the project launched by the Linux Foundation whit the ambition of create an open-source blockchain platform but permissioned, hence “validating and non validating nodes are run by known whitelisted organizations, and where transactors on the network are granted an identity from an issuing authority service on the network” (Le Hors, 2016). Hyperledger’s inner philosophy moves greatly from what Bitcoin is supposed to be, open-source and free from any kind of trusted third party since, again from the whitepaper, “Depending on the purpose of the network, the issuing authority assigns the appropriate level of access that is required to obtain an identity and transact on the network”.

Hyperledger project is backed by the Linux foundation and a consortium of enterprises such as Accenture, ANZ Bank, Cisco, CLS, Credits, Deutsche Börse, Digital Asset Holdings, DTCC, Eris Industries, Fujitsu, IC3, IBM, Intel, J.P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group (MFUG), R^3, State Street, SWIFT, VMware and Wells Fargo (Kerner, 2016).

In June 2016, Hyperledger released its platform named "Fabric". Fabric should be able to run smart contracts, to be modular and able to accept several different technologies in order to be very flexible with regard to its functionalities. Fabrics a permissioned network that protocol is run by peers, which are divided in two different categories[56], validators in charge of running the consensus protocol and non-validators.

Hyperledger's Fabric employs as consensus protocol the Practical Byzantine Fault Tolerance meaning that a blockchain based on Hyperledger, with N nodes, is able to tolerate an f-number of faulty nodes[57] without the remaining N-f nodes suffering from a loose of consensus (IBM, 2016). Unlike bitcoin, Fabric does not have a native currency; since it has implemented the PBFT protocol, it does not have miners neither, here how the protocol works:

- A transaction is sent to one trusted VP.
- The VP broadcasts the transaction to all other VPs.
- All VPs reach consensus (using PBFT algorithm) on the order to follow to execute the transactions.
- All VPs execute the transactions "on their own," following the total order, and build a block (calculating hashes mainly) with the executed transactions.

Non confidential transactions are openly visible by the entire community while confidential ones are encrypted and only whoever hold the encryption key may access them, all the parties and auditors (Akentiev, 2017).

[56] Very peers and not so much peers

[57] From the consensu paragraph f=(N-1)/3

1.2.8.4 Corda

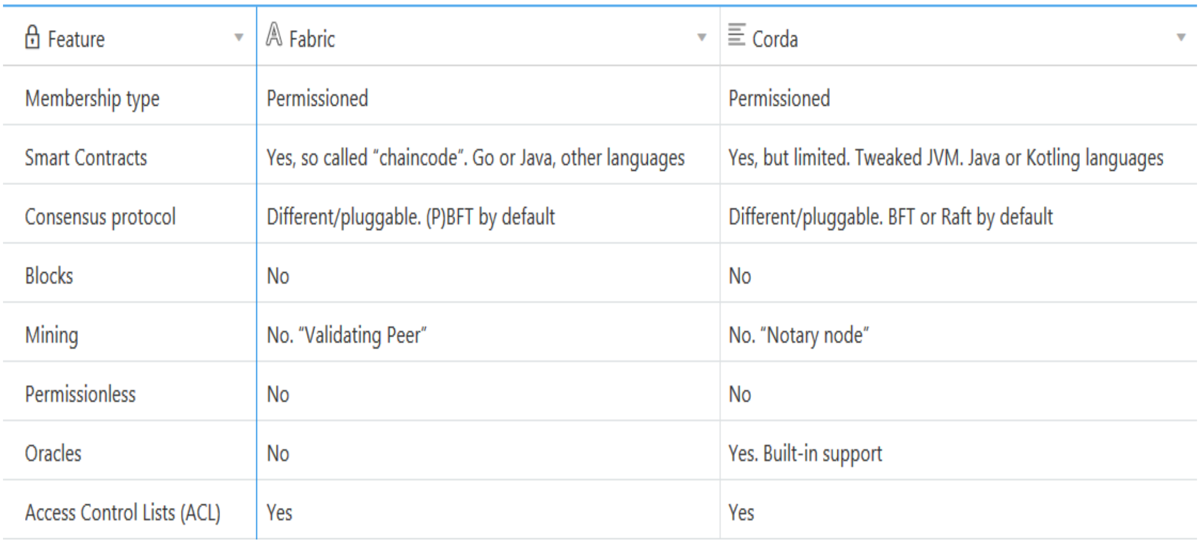
Corda is another DLT platform developed by the R^3 Consortium, which was launched on September 2015 and initially composed by Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan,[9] Royal Bank of Scotland, State Street, and UBS. Then the initial roster has been constantly increase during time with the adjunction of Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, Skandinaviska Enskilda Banken, Société Générale, Toronto-Dominion Bank, Unicredit, Intesa Sanpaolo and many others[58] (contributors, 2016).

R^3 Corda is a distributed ledger for financial services, in particular for record, manage and synchronize financial agreements between different institutions. Corda is a permissioned database "Corda has no unnecessary global sharing of data: only those parties with a legitimate need to know can see the data within an agreement", hence also the consensus of a transaction is reached only with the respect of the parties directly involved in it "Corda achieves consensus between firms at the level of individual deals, not the level of the system" (Brown, 2016). Corda do not allow unnecessary parties to see the content of contracts therefore its validation and consensus protocol is not based on POW, POS, BFT or others but on a "notaries" system that delegates to certain nodes as validators. Corda does not have its own currency and it is not developed as a blockchain at all since "Corda does not organize time into blocks. This is sometimes considered strange, given that it can be described as a block chain system or `block chain inspired'.

Instead a Corda network has one or more notary services which provide transaction ordering and timestamping services, thus abstracting the role miners play in other systems into a pluggable component" (Hearn, 2016). After the release of the technical paper there have been several voices relegating Corda in the field of

[58] In the winter 2016 Goldman, Santanders and Morgan Stanley withdraw from the consortium (Hackett, 2016)

distributed ledgers or shared databases stripping it of its "blockchain" claim (Redman, 2016), (Jones, 2016) and others[59].



Feature	Fabric	Corda
Membership type	Permissioned	Permissioned
Smart Contracts	Yes, so called "chaincode". Go or Java, other languages	Yes, but limited. Tweaked JVM. Java or Kotling languages
Consensus protocol	Different/pluggable. (P)BFT by default	Different/pluggable. BFT or Raft by default
Blocks	No	No
Mining	No. "Validating Peer"	No. "Notary node"
Permissionless	No	No
Oracles	No	Yes. Built-in support
Access Control Lists (ACL)	Yes	Yes

Table 6 A comparison between Fabric and Corda (Akentiev, 2017)

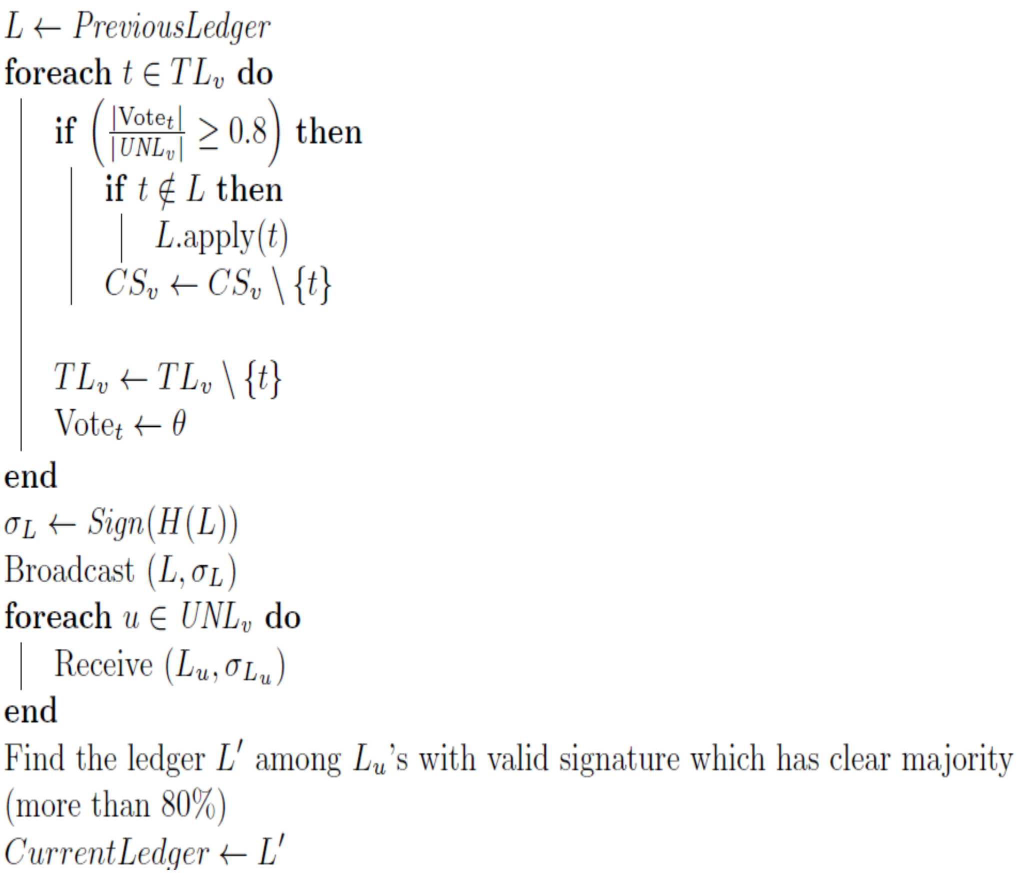
1.2.8.5 Ripple

Ripple is a decentralized payment system based on credit networks, as Bitcoin it aims to bypass several fees and risks typical of the interbank funds transfer processes, which are greater if posed into an international context. Ripple has its own currency (XRP) but in its whitepaper it declares itself "currency agnostic" meaning that it supports other currencies (Rapoport & al, 11/2014). In the Ripple's network, nodes can act like simple users, which do transactions, market makers by offering financial services such as providing liquidity, intra-gateway currency conversion, set up hedge funds, basically acting like a bank that exists only on that blockchain, or a node can be a validator that enforce the consensus protocol.

Gateways are the node of access to the Ripple network, putting or withdrawing liquidity from it. These access points are publicly visible and are required to go through anti-money laundering and know your client procedures (Bradbury, 2016) and (Buterin, Ripple is officially open source, 2016)

[59] Just searching with google "corda is not a blockchain"

Ripple consensus protocol is asynchronous and round based. It implements three different kinds of nodes, users, trackers in charge of gathering information and spreading to the whole network and validators that do the same task as the previous ones but also create their proposal for the next addition to the ledger, similar to a bitcoin's new block but with more information stored in it. At the end of every round, all the validator nodes publish the new version of the ledger. Each node has its "Unique Node List" that is a set of other servers that are called when determining consensus, thus the UNL is a subset of the whole network, for a node its UNL is considered "trusted". If the node receives a new proposal from a server that is not in its UNL it just ignores it. After the collection of proposals, the protocol goes to the consensus phase where each transaction must obtain a super-majority of 80% or more to be considered validated. Figure [31] shows the protocol on a high level pseudo-language (Armknecht & al, 8/2015).



```
$L \leftarrow PreviousLedger$
foreach $t \in TL_v$ do
    if $\left(\frac{|\mathrm{Vote}_t|}{|UNL_v|} \geq 0.8\right)$ then
        if $t \notin L$ then
            $L.\mathrm{apply}(t)$
        $CS_v \leftarrow CS_v \setminus \{t\}$

    $TL_v \leftarrow TL_v \setminus \{t\}$
    $\mathrm{Vote}_t \leftarrow \theta$
end
$\sigma_L \leftarrow Sign(H(L))$
Broadcast $(L, \sigma_L)$
foreach $u \in UNL_v$ do
    Receive $(L_u, \sigma_{L_u})$
end
Find the ledger $L'$ among $L_u$'s with valid signature which has clear majority
(more than 80%)
$CurrentLedger \leftarrow L'$
```

Figure 31 Ripple Protocol consensus algorithm (Armknecht & al, 8/2015)

The definition of any validator's UNL is essential to prevent malicious behavior of other nodes. In the whitepaper of David Schwartz (Schwartz & al, 2014) it is reported that every UNL has to pursue two directions in order to lower moral hazard, lower probability of collusion and being as big as wide as convenient Fig. [32]

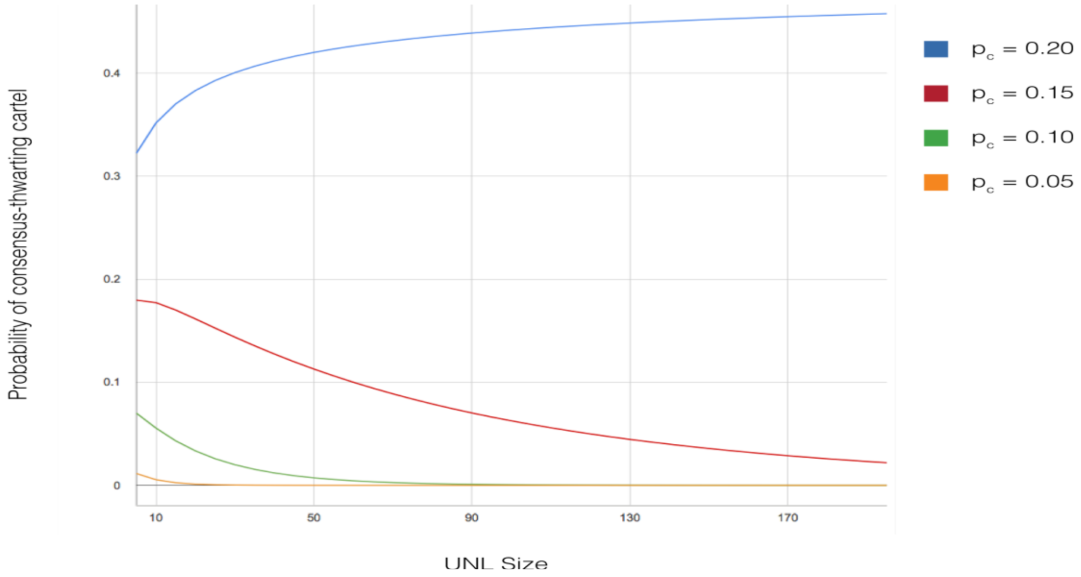


Figure 32 Probability of a nefarious cartel being able to thwart consensus as a function of the size of the UNL, for different values of Pc. (Schwartz & al, 2014)

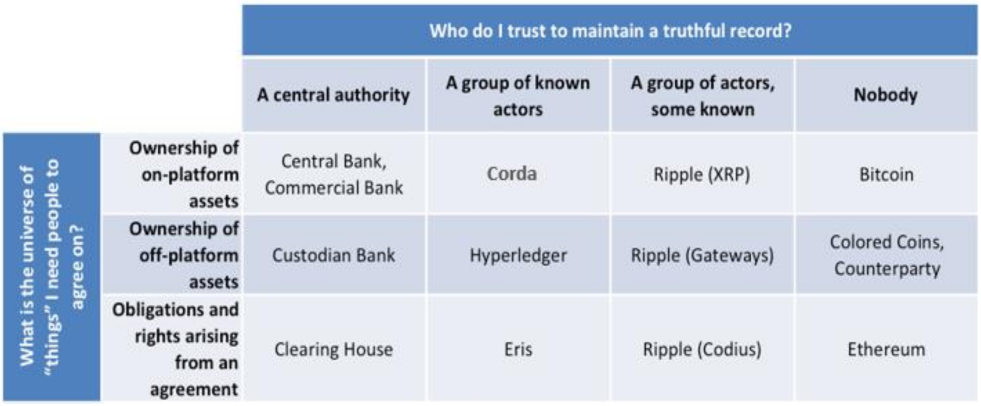
Ripple claims its consensus protocol allow the system to meet a 100.000 transactions per second performance, with a time for the settlement of 3-6 seconds per transaction (Rapoport & al, 11/2014).

The conclusions of Armaknecht's paper "Ripple: Overview and Outlook" suggest that Ripple is not yet a decentralized payment system, on the contrary "the current deployment of Ripple is not decentralized, and offers unconditional power for Ripple Labs to control the fate and security of all Ripple transactions". The consensus protocol has been criticized as well since "the intersection set size between the UNL of any two validating servers needs to be more than 40% of the maximum UNL set size in order to ensure the absence of any fork in the system". This means that taken two different nodes in the network they must have at least 40 other nodes in common in their UNLs to prevent disagreement in the consensus hence provoking discrepancies of their versions of the ledger.

From a white paper by George Samman published by the group Gilbert and Tobin, private shared ledgers have some common features (Samman & Jew, 11/2016):

- Strong, durable cryptographic identification that allows to verify that the author of every modification in the ledger is actually entitled to do so and, in case of investigation it will be possible for many years to retrieve the responsible.
- Distributed so that every entity entitled to participate in the ledger may access its node from whichever locality or datacenter of their choosing
- Full replication is necessary because if a node goes offline it is necessarily to fully recover it.
- Immutability of all transactions using cryptographically proved instruments such as hash functions and Merkle trees.
- Privacy the nature of transactions must be hidden to the entire network but the intended counterparties and the regulator.
- Byzantine fault tolerant consensus protocol are needed to achieve consensus in a private distributed ledger, instead of probabilistic and incentive based approaches.
- High performances in terms of throughput and latency.
- Also fully scalable in case of an increase in the size of the network.

On an online document from Richard Brown's blog, it has been presented a useful matrix to recap and schedule the different platform just saw Tab.[8]



		Who do I trust to maintain a truthful record?			
		A central authority	A group of known actors	A group of actors, some known	Nobody
What is the universe of "things" I need people to agree on?	Ownership of on-platform assets	Central Bank, Commercial Bank	Corda	Ripple (XRP)	Bitcoin
	Ownership of off-platform assets	Custodian Bank	Hyperledger	Ripple (Gateways)	Colored Coins, Counterparty
	Obligations and rights arising from an agreement	Clearing House	Eris	Ripple (Codius)	Ethereum

Table 7 The "who do I need to trust and what am I trusting them about" Matrix (Brown R. G., 2017)

1.2.9 Political and Economic theory of Distributed Ledger Technologies

In this part, I wanted to search literature contributions that tackle economic, political and jurisprudential theories in the light of a technology such as distributed ledgers. Many properties and characteristic of distributed systems could been transposed from a social point of view. For example Bitcoin has been seen from many of the libertarian side of the world as a game changer in their never ending war against governments and taxes, since it transactions are made without third parties and there is no need for names but just for address and public keys in order to perform a transaction (Karlstrøm, 2014) (Ennis, 2016). Because of its properties it has been suggested Bitcoin to be a form of "Heyek money" (Ametrano, 2016) from the Nobel laureate economist Friedrich Heyek and its work about denationalization of money (Heyek, 1974) where it were devised the possibility of a plethora of concurrent private currencies. Bitcoin can be considered private because is decentralized. This might sound contradictory but it has sense if we think about it from the demand side of the table. A person, as a private human being, may choose Bitcoin as its currency not because it has been imposed from a national or international entity but because it has peculiarities that made it decide so. Another open issue is whether Bitcoin is money[60] (Bjerg, 12/2015) (Stephanie & Wnag, 09/2014).

Ferdinando Ametrano in his paper lists three independent functions that a good or a service must have to be branded as money, taken from (Jevos Stanley, 1875):

- Money is a "Medium of exchange". A good is money if it is possible to swap it for something else. This property implies fungibility that is the capability to be substituted in place of another, transportability, divisibility, recognisability, and resistant to counterfeiting.

[60] Perhaps the reader may think that I shifting the focus from DLT to Bitcoin too much but this quarrel about whether cryptocurrency are money is of paramount importance in the light of tokenization, which is already quite common if we think about Ethereum or Ripple.

- Unit of account for the other goods and services. Money is the unit of measurement of relative worth, so it should have a stable value for comparison of prices.
- Store of value for very long periods, even if some degree of volatility is allowed.

Ametrano shows that the first two properties of money are meet by Bitcoin while on the third one the current instability of its price makes very difficult to be used for loans or salaries. An explanation could be linked the impossibility to do monetary policies for Bitcoins, a problem already acknowledged by Nakamoto itself[61]. The problem of lack of external malleability on the supply side of Bitcoin could be overcome with hybrid blockchains or Centrally Banked Blockchains[62] (Danezis & Meiklejhon, 2015) where miners are delegated by the central authority and held accountable for any misbehavior and there is the possibility for central banks to enable active monetary policies. This solution could solve the problem with totally decentralized, full ano/pseudoanonymus blockchains and be more attractive for institutional implementation, without losing advantages from the immutability of blockchains, because full nodes can still download the entire chain noting if there has been modifications. Hence, despite the fact that Bitcoin appears to be Libertarian, a slightly modified blockchain may be a Socialist[63] instrument as Martin White says "while BTC has properties that support Libertarian ideals, there is much about blockchain technology and its development that is directly applicable to various forms of Socialism" (White, 11/2016). In another paper it has been remarked how blockchain can provide society with a higher control over usually shady industries "For the first time, the Blockchain technological innovation has

[61] After having studied several months the bitcoin issue I have come out with the opinion that it is the intersection between currency, valuable materials (gold, silver, diamonds…) and Hi-Tech products, but this is not going to be proved in this dissertation.

[62] Here some Bitcoin maximalist has passed out or it is sending me some curse. For them what I just said is basically blasphemy.

[63] Socialism has been used both as a synonymous of statism and social welfare. Because modifications in the blockchain can actually enhance the control of governments.

given society the option of decentralizing the function of finance and control of the financial industry" (Kosten, 2017).

Independently from what political point of view we want to study this system, many researchers have found interesting to study Blockchain as a possible amendment for "Market's failures" (Probst & al, 04/2016).

1.2.9.1 Market's failures and Distributed Ledgers

Market's failures are forces and condition that prevents the state of "Perfect Competition" or in other words a "Nash's Equilibrium". Because of market's failures the allocation of good and services is not efficient, in a Paretian perspective, hence there is an overall waste of wellness.

Information asymmetries are market's failure because: "some agent in a trade possesses information while other agents involved in the same trade do not. […]when information is asymmetric, prices are distorted and do not achieve optimality in the allocation of resources. […]When two (or more) individuals are about to agree on a trade, and one of them happens to have some information that the other(s) do not have, this situation is referred to as adverse selection. […]The literature on adverse selection then investigates arrangements that allow segmentation of the market according to unobserved quality, i.e. how insurance companies and banks screen their customers with the use of deductibles and collateral requirements […]On the other hand, the case in which the information asymmetry occurs after an agreement is obtained between individuals, is called moral hazard. The framework often used to analyse moral hazard situations is the principal-agent problem, whereby one individual – the principal – wants to hire another individual – the agent – to perform a given task. […]The principal-agent problem framework is now widely used to address issues ranging from public economics to corporate finance. What is quality control if it is not the alleviation of information asymmetries between management and employees by making actions observable, or more precisely contractible? Stock-options, salaries paid in cash and in stocks, merit-based salary increases, are examples of instruments that aim at providing the right incentives to constituencies of an organization, aligning their own objectives with the objectives of stakeholders" (Do, 2017).

In the long quote from a World Bank's paper it has been introduced the concept of asymmetry in the distribution of information. Following a short definition, the author linked to asymmetric information also adverse selection and moral hazard. Both of them have been depicted by two very famous exempla, the second hand cars' sales clerk and the insurances' market.

"Suppose that there are nine different cars, each car having "fair" values, 100$, 200$… 900$ respectively. As the buyer cannot observe quality, owners of low quality cars will always claim they are selling a high-quality product worth 900$. A fair price will then reflect the average quality of the market, in this case 500$. However, under such circumstances, sellers whose cars are worth more than 500$ find such price too low, hence exiting the market. The average price must then drop to 300$, inducing more exits, and so forth. Consequently, at the exception of worst-quality cars worth 100$, no seller is willing to sell a car that a buyer is willing to buy" (Do, 2017). Despite the exemplum, adverse selection is an issue for both buyers and sellers, another classical exemplum is the health insurance industry where adverse selection knocks out of the market good health clients and only sick ones subscribe them. Adverse selection distort the market prior of the transaction[64].

Academic literature proposed market signals as possible solution to adverse selection, in the case of the used cars seller it could be free insurances or for the health insurances one a valid certificate of good medical condition. Another market signal is the quality of seller/buyer reputation.

Moral hazard is the manifestation of asymmetric information a posteriori of the transaction. Moral hazard "moral hazard occurs when a party provides misleading information and changes his behaviour when he does not have to face consequences of the risk he takes" (Nickolas, 2017). Likewise, adverse selection, the first use of

[64] I would like to link the concept of adverse selection to "trust". When an economic subject makes a choice it does trust that is the best option for its utility. Math doesn't imply trust, bitcoin consensus protocol overcome adverse selection in the sense that one of its main characteristic is the trustlessy.

the term come from the insurance world, for instance after having subscribed a car insurance that covers any damage the owner may change is risk appetite because a large share of it is not its burden but it is on the insurer. In this scenario, it is hide to the insurer the behaviour ex-post, so moral hazard is also referred as a problem of "hidden action".

Moral hazard may be addressed with incentivetion for a good ex-post behaviour and malus for a bad one, quite easily, we can link this concept with the periodical variation of an insurance's premium[65].

Hidden information and incentive systems have created during the years an economic branch of studies called "Principal-Agent theory" or "Agency theory" (Mariotti, 2015). Agency theory involves a double party relationship were one (the Principal) delegates work to another (the Agent), who performs it. In this context two different issues arise. The first issue appears whenever the purposes of the two counterparties are not perfectly aligned, therefore it is revered as a "conflict of interests". The second problem is the already defined "hidden behaviour" in the light of the impossibility of a principal to fully assess the agent's work.

The high visibility of assets on a blockchain is a powerful instrument against moral hazard, Professor Yermack says "Blockchain trading of a company's shares would likely reduce the effectiveness of equity-based management incentives. Corporate managers obtain most of their incentives from stock compensation, either from stock options or from restricted shares. Insider trading regulations constrain managers' ability to profit from trades in their own shares. However, an influential literature argues that even when managers trade within the established legal boundaries, insider trading represents a de facto compensation system for them, allowing executives to exploit at least a certain amount of inside information and reap some of the profit associated with the valuable news they create. Blockchain share trading would potentially allow outsiders to observe managers' trades in real time. Investors are keenly interested in knowing when managers receive or liquidate

[65] This concept of incentives for good behaviour has been already introduced in this work of mine talking about rewards for good miners.

equity in their own firms, both because any transaction changes the managers' incentives, and because managers' transactions likely signal private information about the firm. Real-time transparency of trading would expose managers to greater scrutiny by their boards and shareholders, probably causing them to trade less often out of concern of sending adverse signals to the market. The net effect would likely cut into managers' profits from legal insider trading, and firms might have to pay them more to offset this loss" (Yermack, 12/2015).

Another powerful characteristic of Blockchain, his high level of immutability, is another instrument towards better markets addressing again moral hazard and adverse selection. Blockchain would not allow modifications of past information trying to improve the performances of a firm (Lazanis, 2016).

Perfect competition theory has a condition of frictionless transactions, meaning that every exchange occur without ancillary costs. Empirically every transaction is more or less expensive. Transaction costs economics deals with expenses related with every transaction. These costs may arise whether the transaction is made on open market as well as internalise within the same economic entity. Oliver Williamson developed this theory around three main pillars:

- Limited Rationality: Economic agents are rational and they act pursuing the maximization of their own utility, when they are in the condition to do so. Despite this tendency to act rational, there are situations where that is not possible because of the presence of substantial limits, due to the absence of a fully information, and procedural, even if in absence of lack of information still the complexity could prevent from the formulation of a fully logical course of action. Because of these two limit, an economic entity may be forced to spend time and resources in order to make better choices.
- Opportunism of economic agents: Economic agents pursue their own wellness, therefore in presence of information asymmetry logic moves them towards an opportunistic behaviour, hurting the wellness of other counterparties. Since all the parties involved into a transaction are rational and aware of the possibility that their lack of information might be exploited

by others they are again forced to employ resources in order to defend themselves against this eventuality.

- Specific relationship investments: Within an economic transaction, one or all the parties may be forced to spend money investing in assets that have the capability of creating profits only or partially within that specific business relationship, outside it they would be sunk costs.

Limited rationality, opportunism and relationship specific investments increase their effects depending on the frequency of which transactions take place, the level of specificity of a particular transaction and its complexity and uncertainty (Williamson, 1973) (1975) (1979) (1983). Davidson, De Filippi and Potts in their "economics of blockchain" state that smart contracts and their combination forming a Distributed Autonomous Organization may pose a limit to the generation of transaction costs (Davidson, de Filippi, & Potts, 05/2016). Their statement poses in trust the very reason transaction costs arise and, since some consensus protocols may be designed to implement trustlessnes, distributed ledgers can overcome the problem.

All this biases led a party to exploit a temporary situation of advantage at the price of the others' returns, whether is an asymmetry in the information possession or the appropriation or waste of economic resources due to the presence of transactional costs or externalities. Nevertheless, there is always the, more or less scious, intention of a party to exploit a market failure, while trying to prevent the same kind of behaviour from its counterparties. The dynamic described can be called a "game", the field of study of games is called "game theory". Bitcoin's proof of work could also been seen as a transposition of many concepts from game theories, PoW and incentives in the form of newly minted coins force participants to play in the direction of strengthening the protocol hence Bitcoin. In addition, relationships between different miners have been translated according to a gaming standpoint (Schrijvers & al, 2016) (Benjamin Johnson, 10/2014).

Finally academic's interest towards distributed ledger technologies and market's failures focused on externalities. Externalities are a particular kind of effect created both by the production and by the consumption of a particular good/service. Externalities are considered a failure because they are not transact on a market, for this reason they are also referred as a case of "missing market".

Academic literature revised for this economic section state that Bitcoin[66] increase its value functionally to the size of its user bases, this effect is known as "network externality" or "network effect". Ernie Teo noticed Cryptocurrencies present strong network externalities[67]. Also the strong influence of this effect on the value increase as well the return for all the complementary services and goods, such as miners, exchanges, wallets makers, developers and so on. Of course, these ancillary entities are incentivised to create more value by proposing innovation and this triggers a virtuous circle (Teo, 2015).

In his article, Teo used a framework devised in another work by Evans and Schmalensee where network effects are divided between direct and indirect. Direct network externalities are the added value for the participants brought by the increase of the network base with other similar users.

The condition for potential new adopter to enter the network is:

$$V_i\,[N(t)|\alpha_i] - \theta_i - P \geq 0 \text{ or } \Omega_i \equiv V_i^{-1}(\theta_i + P|\alpha_i) \leq N(t)$$

With V the value of joining the network for the i-person, that at time t has N size, α is the intrinsic value of that particular network for that i-person, θ is the cost of participating and P is the price charged[68]. Ω is the inverse utility function that helps to find the minimum number of participants in the network (Evans & Schmalensee, 2010).

For Teo, Bitcoin reached its critical mass, through mining, during the first year. This could be the reason why mining reward was so hefty at the beginning and the

[66] Unfortunately the vast majority of papers dealt only with Bitcoin and not with DLPlatforms in a broader sense. But still I assume that most of the conclusions can cope more than sufficient for all distributed ledger platforms.

[67] Meaning that, compared to other objects, the addition of a new user to the network increase substantially the overall value of it.

[68] Therefore θ are transaction costs to switch and adapt to the new network.

target difficulty of the proof of work so low[69]. Bitcoin's ability to reach its critic volume in just one year could be related to the fact it had not such a competition, basically exploiting the "first move advantage" (Gandal & Halaburda, 2016)

Indirect network externalities refers to the increment of value for the network's partecipants due to the increase of the users' base of one of its ancillary network, for cryptocurrencies miners, developers and so on.

In the conclusion of his work, Teo posed as key success factor for a crypto currency the reward system for miners. This conclusion creates a condition of trade off between the possibility of not paying, in bitcoins' transactions, any fee and the necessity to attract as much miners as possible. That is because ancillary services to the Bitcoin network do not benefit from direct network externalities, since miners are in competition one with another. I could suggest that the loss of value connected to inflation when new coins are mined and transaction fees have the same essence of a "piguvian tax", which is a solution proposed to repel effects of negative externalities[70] (Sandmo, 2017). Other researchers again backed the hypothesis that Bitcoin value is driven mostly by its own popularity (Polasik & al, 10/2014). I would like to cite again Ametrano's work that tends to give more credits also to the intrinsic value of Bitcoin as a probable substitute of Fiat currencies (Ametrano, 2016).

1.2.9.2 Jurisprudence and rule of distributed ledger technologies

This part was mainly covered by Institutional papers more than academic one, which are currently much more interest in the technological, mathematical and economic aspects of the distributed ledger phenomenon[71]. I would suggest that one

[69] "stroke of genius"

[70] This is just a conclusion of mine without any claim of veridicity.

[71] At least judging on the base of what I have found during this review.

reason lays on the political perspective, at least, of Bitcoin that, as has been reported at the beginning of this chapter is strongly libertarian oriented therefore allergic towards regulations form outside the free market[72].

In a paper from February 2016, the European Commission proposed to proceed using a "Smart Regulation" approach: "The key to smart regulation in such an environment of dynamic innovation is for the regulator to develop sufficient capacity, including technical expertise. Pre-emptive and heavy-handed regulation that would stifle growth should and can be avoided. However, such a smart regulatory regime based on analytical excellence and proportionality must not be confused with light-touch regulation: rapid and forceful regulatory measures need to be part of the toolkit in order to address risks before they become systemic if and when appropriate. In order to assure the regulatory capacities needed for this approach, the rapporteur calls for the creation of a horizontal Task Force DLT to be set up under the leadership of the Commission" (von Weizsäcker, 02/2016).

The European Securities and Markets Authority (ESMA) issued on June 2016 a discussion paper where it asked to academic and corporative audience to address several aspects of implementing Distributed ledger technologies for institutional markets and exchanges under its jurisdiction. In chapter 4 section 3 of this paper, it reported three potential "Regulatory and legal issues":

- "The capacity of the DLT to fit into the existing regulatory framework may limit its deployment".
- "Legal issues, such as the legality and enforceability of the records kept on the DLT, also need to be carefully considered. Differences in securities and company laws across the EU may also interfere with a wide deployment of the DLT in securities markets in the EU".
- "Finally, supervising a DLT 'network' might be more complex than supervising central market infrastructures, in particular considering that the

[72] All these considerations are free to be picked by anyone willing to increase the knowledge around this topic. Perhaps I will do part of it.

> different nodes might be established in different jurisdictions and subject to different privacy, insolvency and other requirements".

In Chapter 5 section one, ESMA shows its concern about the possibility that "DLT could be exposed to the risk of money laundering and terrorist financing activities, notably because the use of public/private keys could make it easier to conceal identities and to hide the history of transactions".

Finally, Chapter 6 introduces the possibility of permissioned platform where only certain entities, which are complainant with future requirements, can perform. Also sections six highlights how these platforms should be conceived around already existing regulations such as: "European Market Infrastructure Regulation (EMIR), the Settlement Finality Directive (SFD), the Central Securities Depositories Regulation (CSDR). CSDR). Other pieces of legislation such as the Markets in Financial Instruments Directive (MiFID), the UCITS Directive and the Alternative Investment Fund Managers Directive (AIFMD) for the record keeping of ownership are also discussed. Other pieces of legislation such as the Securities Financing Transaction Regulation (SFTR), the Directive on Financial Collateral Arrangements, the Market Abuse Regulation, the Anti-Money Laundering Directive or the Short Selling Regulation could be relevant as well but are not discussed in this paper. Notwithstanding the binding regulatory requirements likely to apply, some principles, like the CPMI-IOSCO Principles for Financial Market Infrastructures, may also provide useful guidance" (ESMA, 06/2016).

The call from ESMA received a strong response from the enterprise world with tens of replies, a more timid response arrived from academic experts and from other public entities. From these responses, it was possible to define an initial set of regulatory issues provided, mostly, by the corporate side.

- Privacy issue. Definitely the most reported issue among all the responses is privacy. "The open nature of DLT gives rise to issues surrounding the confidentiality of data between actors, such as product positions, which will need to be sufficiently protected. Further, it is possible that the identity of the participant could be derived – not withstanding encryption of the identity of the participant – by analyzing the content of the account (which would typically be unencrypted)" (Sukumar, 2017) "is indeed one of the more relevant and critical issues that need to be addressed, especially when it comes to managing private client information. This places great emphasis on the continuous development of sophisticated encryption techniques to constantly protect the participants and their data" (XNotes, 2017). Other responses provide solutions to this matter, still reckoning the entity of the issue, like "While privacy issues remain significant, the development of data tokenization techniques can help to provide anonymity and maintain privacy for the users of DLT. Using such methods, data is tokenized into something that only the participants relevant to the transaction would recognize. The real interest of the token is to add a layer of security on the top of the secure blockchain cryptographic technique. The details of the document are partially hidden on the blockchain and a full read access to third parties might only be given upon special approval from the supplier or the client" (XNotes, 2017) or "With regard to privacy issues, Corda is designed such that not all data is shared with every node, but rather is only shared to the extent that it needs to be" (R3Cev, 2017).

- Another regulatory issue highlighted in several responses was the reconciliation of the worldwide nature of a distributed ledger with the specific geographical jurisdiction of public agencies such as ESMA itself or the SEC for instance (Reply, 2017).

In the paper "Distributed Ledger Technology: Beyond Blockchain" issued by the UK chief scientific adviser it is highlighted how the problem concerning regulation over this kind of technology has to be addressed from both jurisprudential as well as technical perspectives. It is described that legal code is "extrinsic", meaning that rules can be broken and, after that, consequences are triggered. On the other side computer code is "intrinsic", hence a hole in the code prevents from going on because an error is returned.

The authors then proceed explaining that in the current state, where mostly of the procedures are already digitalized but held on private databases, code have nearly no influence over regulatory procedures and legal perspective is the sole perspective inquired. The change of paradigm proposed by Distributed Ledger Technologies may impose to the regulator a much more integration also of the "mathematical" perspective. Bitcoin is brought as the instance for an organization where the mathematical design made law nearly inconsequential[73].

At the end of the chapter, there are two propositions of how to regulate distributed ledgers from the legal point of view and the other from the code one. From a classic vision of regulation, distributed ledgers should be controlled by addressing directly the nodes of the network[74]. This approach of course is more or less feasible depending on the level of anon/pseudo anonymity of the network.

The new approach for regulate this technology would consider the transposition of the will of the regulator directly into the source code by addressing the private developers or creating itself the distributed network where it can act as a super node[75]. Regarding this matter Clack and Bakshi proposed two ways of enforceability of contracts stored on distributed ledgers (Clack & Bakshi, 08/2016):

- Traditional enforcement is disputes resolution through arbitration or at a court of law. That is possible only if there is a government recognition of the validity of a contract loaded on a blockchain. A court may impose the exchange of the underlying or the payment of it, confiscate physical assets, fines a counterpart or deprive it of liberty. Traditional clearinghouses can take in charge the management of a collateral or the resolution of a contract and so on.

[73] For everything written inside the code. Legislation could still enforce its authority through people.
[74] It has been reported in the paper the case of "BitLicense, issued by the New York State Department of Financial Services to businesses offering digital currency services to New York residents2. The deadline for businesses to obtain the license was 8 August 2015, and unlicensed service providers can be penalised".
[75] For example knowing the direct affiliation of every address.

- Nontraditional enforcement of a contract may happen “on chain”, the smart contract itself may manage its own enforcement without the need of the trusted third party. This ability may create tamper resistant contracts, meaning that the execution of the contract will always go according to its code, assuming no fault in the implementation of it nor in the hardware and infrastructures.

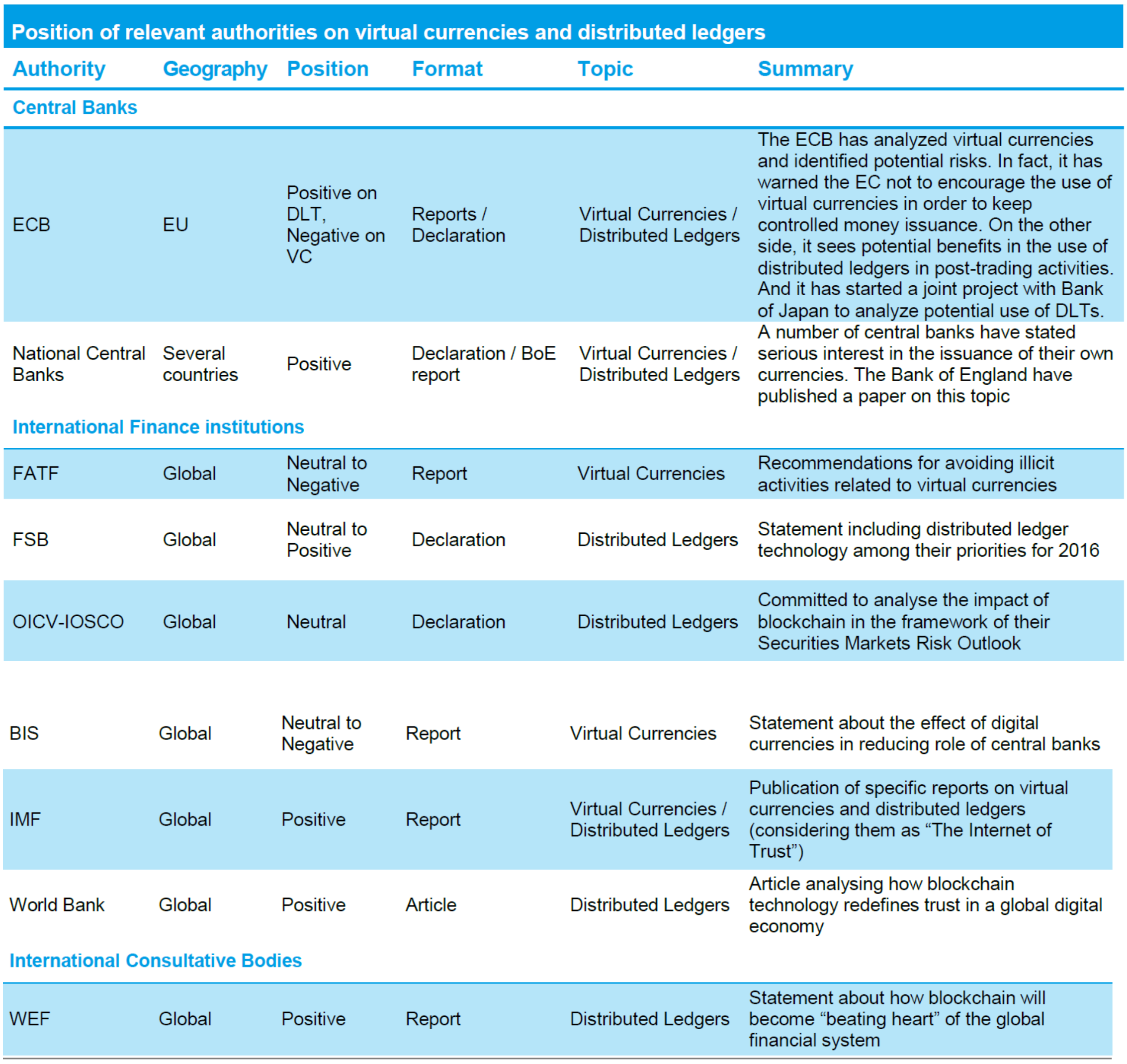
One limitation to smart contract automatic enforcement of their covenants is their current inability to monitor events off-chain. For instance if a smart contract has to make a payment of a certain amount of coins, which are available, at a certain moment in time then the program can detect the current time just looking at the previous block, which has reported its generation instant. In this case, the information can be obtained directly on the same ledger of the contract. Another contract may be triggered by another event, which has manifestation off chain, for example, the current value of a stock or the actual physical underlying of a derivate (Braendgaard, 2017).

For the example above of a stock’s value, a smart contract can comprehend feeds provided by oracles.

Despite not being academic nor institutional, I found quite interesting and well posed a report from BBVA research that released an exhaustive working paper in December 2016 about the current state of international regulation of distributed ledgers (Cermeno, 12/2016). In this work, it has been filled a table with the dispositions and summaries of the intents of all the most influent regulatory authorities towards cryptocurrencies and distributed ledgers Tab.[9]

Position of relevant authorities on virtual currencies and distributed ledgers

Authority	Geography	Position	Format	Topic	Summary
Policymakers					
European Parliament	EU	Neutral to Positive	Report / Taskforce	Virtual Currencies / Distributed Ledgers	Hands-off approach to regulating blockchain technology. Creation of a task force to analyse it
European Commission	EU	Neutral	Directive / Taskforce	Virtual Currencies	Inclusion of virtual currencies players in the AML Directive. DLT workstream inside the Financial Technology Task Force
US Senate	USA	Neutral	Letter to regulators	Virtual Currencies / Distributed Ledgers	Request to regulators for guidance on these technologies
US House of Representatives	USA	Neutral	Non-binding resolution	Virtual Currencies / Distributed Ledgers	Resolution calling for a national technology innovation policy including digital currencies and blockchain technology
US Congress	USA	Positive	Study group set-up	Virtual Currencies / Distributed Ledgers	Creation of a caucus (study group) dedicated to bitcoin and blockchain
State Governments	Several US states	Positive	Regulation	Virtual Currencies / Distributed Ledgers	New York, North Carolina, Vermont and Delaware have promulgated specific regulations
Financial Authorities					
EBA	EU	Negative to neutral	Reports	Virtual Currencies	Recommendation to banks not to deal at all with virtual currencies, and amendments to the EC decision to include virtual currencies players in the AMLD
ESMA	EU	Positive	Public Consultations	Virtual Currencies / Distributed Ledgers	Consultations on investment using virtual currency or DLT and on DLT applied to securities markets
FinCEN	USA	Neutral to Negative	Report	Virtual Currencies	Guidance to avoid illicit activities through the use of virtual currencies
CFPB	USA	Neutral to Negative	Report	Virtual Currencies	Statement about big issues have yet to be solved regarding virtual currencies
OCC	USA	Positive	Report	Distributed Ledgers	Statement about how DLT has the potential to transform how transactions are processed and settled
CFTC	USA	Positive	Declaration	Distributed Ledgers	Statement about how blockchain may give regulators transparency
SEC	USA	Neutral	Declaration	Distributed Ledgers	Statement about the commitment of the agency in actively exploring blockchain regulation
Federal Reserve	USA	Positive	Declaration / Report	Virtual Currencies / Distributed Ledgers	Statement about how blockchain may represent the most significant development in many years in payments, clearing, and settlement. In the context of payments, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography
FCA	UK	Positive	Declaration / Sandbox Initiative	Distributed Ledgers	Statement about considering approving blockchain-based firms into their Sandbox Initiative (finally, 9 out of 16 approved firms use DLT)



Position of relevant authorities on virtual currencies and distributed ledgers					
Authority	**Geography**	**Position**	**Format**	**Topic**	**Summary**
Central Banks					
ECB	EU	Positive on DLT, Negative on VC	Reports / Declaration	Virtual Currencies / Distributed Ledgers	The ECB has analyzed virtual currencies and identified potential risks. In fact, it has warned the EC not to encourage the use of virtual currencies in order to keep controlled money issuance. On the other side, it sees potential benefits in the use of distributed ledgers in post-trading activities. And it has started a joint project with Bank of Japan to analyze potential use of DLTs.
National Central Banks	Several countries	Positive	Declaration / BoE report	Virtual Currencies / Distributed Ledgers	A number of central banks have stated serious interest in the issuance of their own currencies. The Bank of England have published a paper on this topic
International Finance institutions					
FATF	Global	Neutral to Negative	Report	Virtual Currencies	Recommendations for avoiding illicit activities related to virtual currencies
FSB	Global	Neutral to Positive	Declaration	Distributed Ledgers	Statement including distributed ledger technology among their priorities for 2016
OICV-IOSCO	Global	Neutral	Declaration	Distributed Ledgers	Committed to analyse the impact of blockchain in the framework of their Securities Markets Risk Outlook
BIS	Global	Neutral to Negative	Report	Virtual Currencies	Statement about the effect of digital currencies in reducing role of central banks
IMF	Global	Positive	Report	Virtual Currencies / Distributed Ledgers	Publication of specific reports on virtual currencies and distributed ledgers (considering them as “The Internet of Trust”)
World Bank	Global	Positive	Article	Distributed Ledgers	Article analysing how blockchain technology redefines trust in a global digital economy
International Consultative Bodies					
WEF	Global	Positive	Report	Distributed Ledgers	Statement about how blockchain will become “beating heart” of the global financial system

Table 8 Non-exhaustive summary of initiatives and pronouncements by different authorities about Cryptocurrencies and Distributed Ledgers (Cermeno, 12/2016)

The successive chapter of the paper is dedicated to devise the most probable solutions that could be adopted by a regulator.

The first option proposed is the already proposed presence, within the network, of a “super” node held by the regulator. This node will have the access to every, otherwise, reserved information concerning the other participants. The author assessed as improbable to see this solution implemented because the network aims to be international while regulators have authority only within their country for the most part or eventually, like for the ESMA or the BCE, over a community. This would inevitably leads towards the creation of several regional distributed ledgers, which is contemplated in the second option.

The second option devised in the paper implied again the presence of several regional consortia, this time regulators may preside nodes within any of which in order to gain visibility over their subjects. In addition, regulators would have a presence also on an exclusive ledger where they would be able to share information Fig. [33], this "super"-ledger would be connected with any of the others thorough protocols like the Interledger[76].

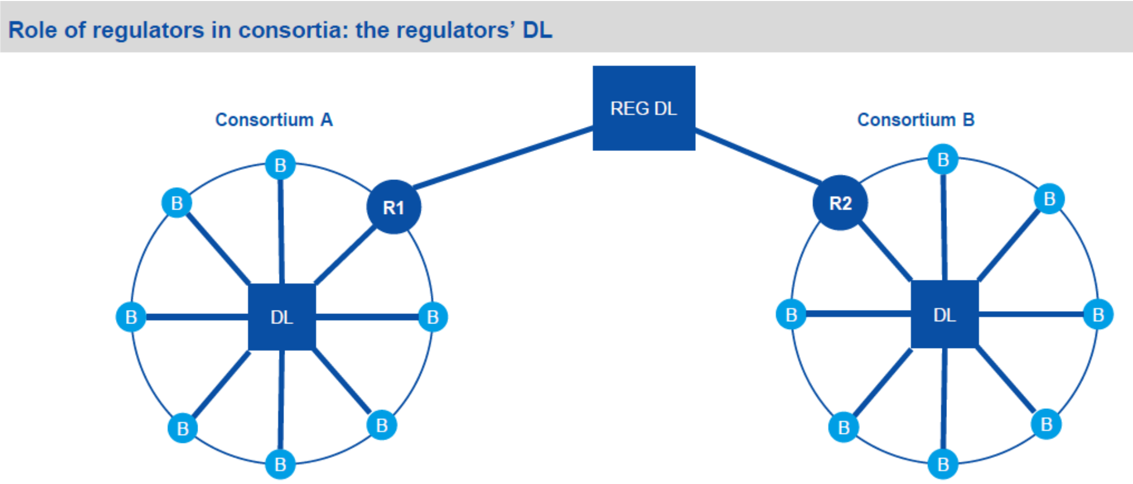


Figure 33 Consortia and the super-consortium (Cermeno, 12/2016)

The third and final possibility presented in the report is to allow regulators to participate to different consortia, hence a single consortium may have one or more nodes hold by institutional regulators. Still every regulator would be able to have a complete view just upon its own "subjects" and nothing more. Then information gathered by a regulator would be stored on its own ledger and shared, on a higher level, between its international peers through the already introduced "super"-ledger Fig [34].

[76] Interledger is a protocol conceived in order to make possible the safe transfer of information across different ledgers. The fundamental idea beneath it is to use escrows in order to allow users to move an asset on the ledger of their preference.

It is the report’s author opinion that this third option is the most likely to be adopted when or whether the distributed ledger will be adopted as a standard.

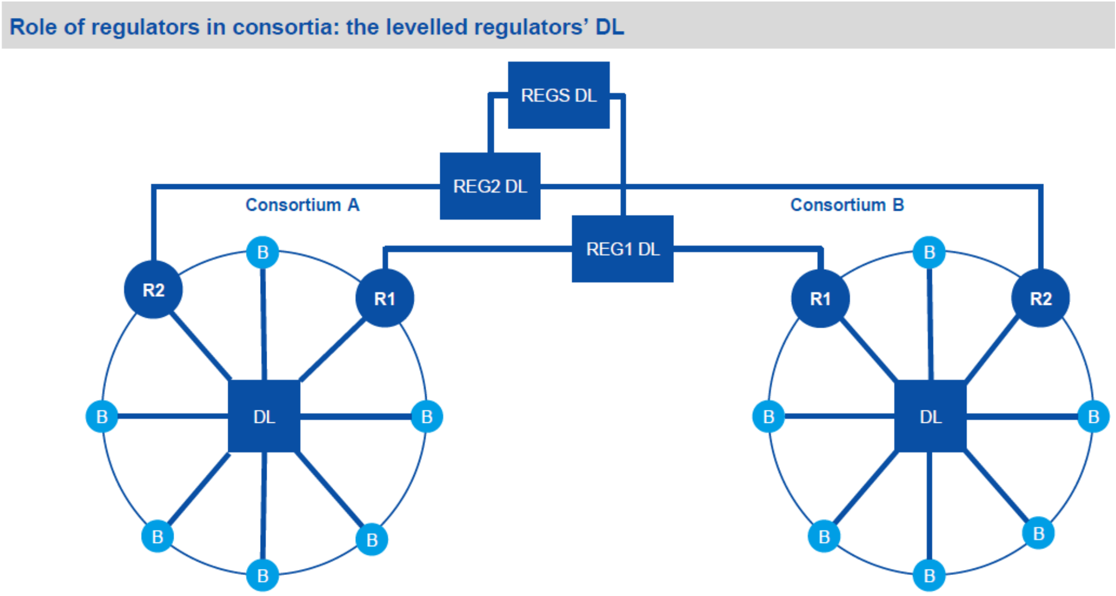

Role of regulators in consortia: the levelled regulators’ DL
REGS DL
REG2 DL
REG1 DL
Consortium A
Consortium B
R2
R1
R1
R2
DL
DL
B

Figure 34 Third option (Cermeno, 12/2016)

This section, if we ever going to devise a concept for a system based upon DLTs, provides us with the guidelines to be compliant with what could be the future regulatory framework. This is as important as the technological feasibility, otherwise we could end up with a perfect concept that cannot be actually implemented outside its sandbox.

1.2.10 Future and actual applications of Blockchain

1.2.10.1 Record keeping

After this introduction about Distributed ledgers and Blockchains, we can already draw a preliminary conclusion about what this paradigm actually is. Starting from the definition of notary for the Italian law: “I notari sono ufficiali pubblici istituiti per ricevere gli atti tra vivi e di ultima volontà, attribuire loro pubblica fede, conservarne il deposito, rilasciarne le copie, i certificati e gli estratti” (Notaries are public officers in charge of the reception contracts among the livings and last wills, proving their validity, storing them safely, providing valid copies, certificates and abstracts) (d'Italia, 1913). From this definition we can see how a distributed ledger is fundamentally nothing more than a decentralised and secure notary system.

This statement has been reviewed by a work of Lemieux. In this contribute the author studied the value of Factom. Factom is a service that relies on the Bitcoin's blockchain extending its potential outside the transaction field. Basically, Factom receives entries by its users, then it assembles these inputs into blocks and after a certain period, it sends them to the Bitcoin mining pool to carve said inputs into the blockchain Fig. [35] (Snow & al, 2017).

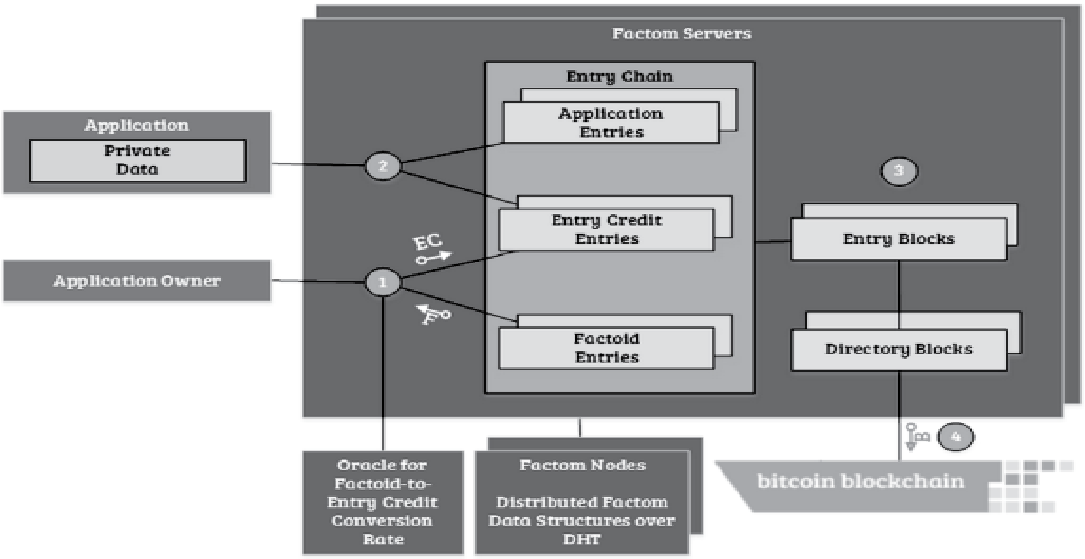


Figure 35 Factom ecosystem (Snow & al, 2017)

The conclusions of Lemieux work are quite sceptic about the real possibility of blockchain for recordkeeping. In particular, it doubts about the reliability of this solution because of the centralized, in the Factum system, entry point[77]. On the other side, the analysis recognizes authenticity as the core offer and main opportunity of blockchain, but still it clinch the importance of security in order to prevent any kind of breach in the system. Long term preservation is another key

[77] About the critic of centralization of the Factum system, in the paper "Factom Ledger by Consensus" it has been declared that the protocol which is used to built the "entry" blocks is decentralised since the building is delegated randomly among the "federated servers" community.

issue that might disenable blockchain and Factum that relies massively on it, from being a viable solution for a corporate grade recordkeeping system. This is because in any moment a new proposition can appear and destroy the value of Bitcoin, hence stopping the mining process the records would suddenly exposed to attacks (Lemieux, 2016).

ESMA, after having analysed the feedbacks from its call for opinions, published in February its own report where it states clearly its positive sentiment about the benefit of a record keeping system for securities' ownership based upon a distributed ledger system. This position is further supported by the possible implication of an automatized post-trading management system that would be feed by said notary. The report continues pointing out the lack of harmony within the EU financial institutions, which causes the necessity of several intermediaries, custodians, registrars, notaries, depositaries and central securities depositories. This conviction is founded upon the sentiment of the ESMA and the broad agreement raised among feedbacks (ESMA, The Distributed Ledger Technology Applied to Securities Markets, 02/2017).

Systems such Bitcoin's blockchain, cannot hold an entire contract because of the limit in the size of its blocks, but it can store a transaction where it has been reported the hash of the said contract signed by the public keys of all the parties involved. This would consist in a proof of existence of the contract in the specific terms agreed, we saw as it would be impossible to replicate the hash while changing the content of it (Crosby & al, 2015). Massimo Bartoletti and Livio Pompianu studied the OP_RETURN instruction which allows to save arbitrary data directly on the Bitcoin's blockchain, as stated before this system allows whoever to prove the existence of a certain document at a certain moment, thanks to the timestamping protocol of the Bitcoin mining system (Bartoletti & Pompianu, 03/2017).

I would risk to state, at this point, that this is the real nature of blockchains and distributed ledgers. The further applications this work is going to analyse are nothing more that direct consequences of the notary/record keeping properties of them. To use a terminology taken from the innovation management course:

"Timestamping and proof of existence is the radical innovation, what follows in just kaizen". Nevertheless, what follows is quite intriguing as well.

1.2.10.2 Corporate Governance

"Corporate governance is the system of rules, practices and processes by which a company is directed and controlled. Corporate governance essentially involves balancing the interests of a company's many stakeholders, such as shareholders, management, customers, suppliers, financiers, government and the community. Since corporate governance also provides the framework for attaining a company's objectives, it encompasses practically every sphere of management, from action plans and internal controls to performance measurement and corporate disclosure" (Investopedia, Corporate Governance, 2017).

Corporate governance is highly influenced by information asymmetries, in particular when they assume the form of an agency problem. In an article of Jie Cai it has been proposed how the impact of this market's distortion influences the choice of which mechanism of governance is going to be implemented. These mechanisms are the intensity of board monitoring, the exposure to market discipline and the CEO pay to performance sensitivity. For intensity of board, monitoring the author means the ability of whoever is in direct charge to press the governance to do so in complete absence of conflicts of interests. Therefore, the authors as proxy of this variable took into consideration the "board index". The board index "The board index increases in the percentage of independent directors, the separation of the CEO and the chair, the presence of a lead director, the existence of audit, nomination, compensation, and governance committees, and the percentage of independent directors on audit, nomination, and compensation committees; the index decreases in the size of the board". For the exposure to market, discipline is meant how the fear of a take over from an external agent on the market boost the implementation of governance because of the fear of a management turnover, after an acquisition. Finally, the CEO pay for performance sensitivity is the variation of the CEO's benefit with regard to the increase or decrease of the stocks' value of the firm. The more this retribution is sensitive the more the board is commit to the value for shareholders the more a good governance is supposed to be implemented. From the asymmetries standpoint the paper listed several variables to indicate to which extend shareholders may be sheltered from them. The size of the firm, the larger they are the fewer asymmetries there are going to be, the expenditure in R&D, especially for innovative firms, the number of shareholders and other variables. The result of this research is that firms with greater asymmetries tend to be disciplined more by been exposed to the market and by the sensitivity of the CEO's benefits than from the internal board[78] (Cai & al, 2015).

I've already introduced the work of professor Yermack (Yermack, 12/2015) previously, in the same article he was quite confident that a system based upon distributed ledgers were more likely to emerge first in emerging markets, because of the inadequacy of the current infrastructure, because of the mistrust of the market towards its regulators and because of an high penetration of information technology. These three forces are well present also into the crowdfunding environment, hence this work of mine assumes the prediction made by professor Yermack has merit also within this industry. From the corporate governance stand point Yermack underlined several benefits connected to an enhanced transparency:

- Greater transparency of ownership: For a company which has its stocks listed on a distributed ledger all intended people might be able to witness all the movements of that firm's property. In addition, managers who holds shares of their own company would not be able to liquidate their position without sending a strong signal to the markets about the healthiness of the firm.
- Improvements of assets' liquidity: Because of the potential of Distributed ledgers to reduce both time and costs of transactions they are seen as a possible enhancer of market liquidity, which currently requires an average of three business day to complete a trade.

[78] All this just to justify the importance of a lively market for highly shady firms, just as start-ups are.

- Entitled shareholders would be able to cast their votes on a permissionless public blockchain in order to be sure that their vote will not be subjected to forgery, because it will last in uncountable number of different memories and because the mining will be done by miners randomly chosen by the protocol, therefore not connected to any particular interest.
- Real Time Accounting: On a distributed ledger bestowed with anti-tampering capabilities it would be impossible change ex-post a record without having to broadcast the change to the whole network, without being able to overwrite the previous information nevertheless. Even if just the hash of a certain document were stored on the ledger, it would be quite difficult to store it entirely, a change in the original copy would hash a completely different result, this would eventually trigger an in depth further investigation.
- Smart contracts: After the "sign" of a smart contract and its upload to the blockchain, it would be impossible for all the parties to act against that document. The willingness to accept to enter into a smart contract would be a strong signal from the more powerful counterpart not to behave in an opportunistic way. In addition, Smart contracts on distributed ledgers with their own currencies would allow the parties to create a set of rules, like covenants, payments schedule, escrows and so forth just to prevent any kind of misbehave.

1.2.10.3 Blockchain in cross border payments

Blockchain, as a peer-to-peer system with a cryptocurrency and a proof of work, was borne with Bitcoin and thrived in the early ages after 2009 with a huge amount of other cryptocurrencies, mostly failed soon after their launch with no market value nor maintenance (Faggart, 2017) (Isle, 2017) (Alcoins.com, 2017). Many other altcoins are rip off bitcoin, meaning that someone took the source code and modified it implementing some feature, while others are developed from zero and run their own blockchains[79].

[79] Many of the most promising or followed cryptos will be detailed in the chapters ahead.

According to a report from Bain (Williams & al, 2016) payments, in particular international ones, is the single most profitable field for blockchains with a market of 150-200 billion US Dollars in revenues and many sources of frictions during these processes.

Number of different players involved in a cross border payment, such as in Fig.[36] increases both times and costs. Many institutions do not share common standards therefore resources are wasted during harmonization procedures (Park, 2006). The presence of many intermediaries in a serial system increases also the chance of a failure in the process; just one entity going into downtime would jeopardize the entire process requiring longer latencies.

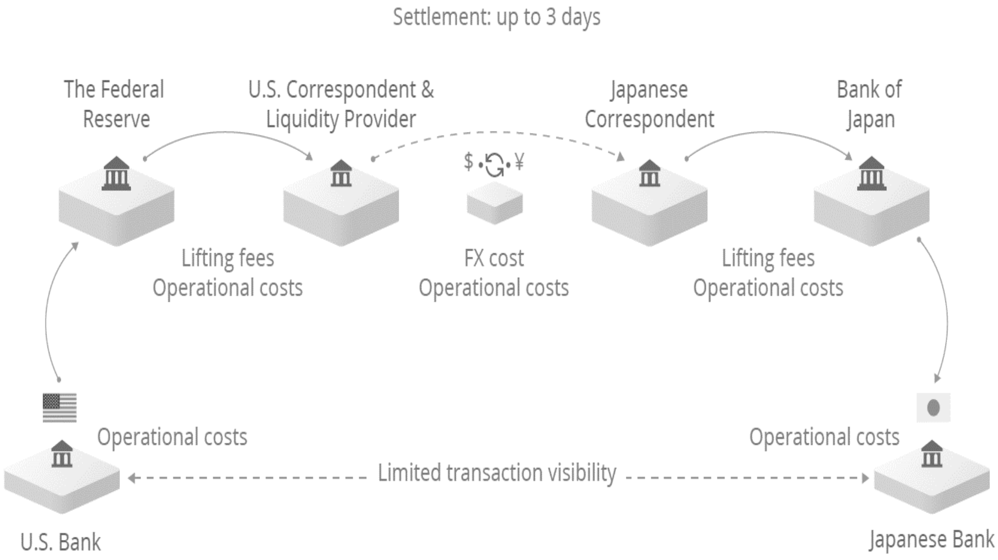


Figure 36 Representation of a cross border payment (Ripple, 2016)

In this respect blockchains, such as Bitcoin in the first place, allow for a rapid and flawless movement of value. Fundamentally because a proper blockchain has the ability of reaching a “distributed consensus”, meaning that there is not a handful of third trusted party but, in Bitcoin and others, the whole network is involved in recognizing every single transaction. This of course create a huge redundancy, which prevents any kind of failure and increases several times the security of the assets (Nakamoto, 2009).

1.2.10.4 Escrow and custody

Escrows is, quoting the Wikipedia's 1definition: "a contractual arrangement in which a third party receives and disburses money or documents for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties; or an account established by a broker for holding funds on behalf of the broker's principal or some other person until the consummation or termination of a transaction; a trust account held in the borrower's name to pay obligations such as property taxes and insurance premiums" (contributors, Escrow , 2017).

This service should eliminate for all parties the risk of frauds. Unlike banks, custodians cannot trade the underlying of an escrow agreement or use it as a safekeeping for their own purposes. For this service, and also because they can be charged of the wellbeing of the underlying, the trusted third party is usually compensated with a percentage of the asset's value. In the light of the precedent definition, I would also add the institution of the clearinghouse, which acts like the counterparty of all the parties that is in charge of the collateral management and the payment day by day of contracts, usually in the futures' market.

On a Distributed ledger it would be possible to implement escrows agreements and forth without the direct delegation of it to a trusted third party but just implementing a smart contract which will eventually run by a party chosen by the consensus protocol when the conditions written on it are met. The presence of a distributed ledger may help reducing the need for intermediaries and costly reconciliation procedures. Escrows may also be used for transferring value from a ledger to another, just by sealing the asset on the sending while creating a new token for it on the receiver and vice versa whether we want to transfer again the assets on the original one (Mills & al, 2016).

Starting from an idea devised into the paper of Peters and Panayi (Peters & Panayi, 2016), a multi signature escrow system may also be beneficial for a conflict resolution, for example two parties may agree on a sell just because one party escrowed the payment. Now the money within the escrow are definitely out of the reach of the buyer therefore the seller can authorize the shipments of the goods. After the completion of the shipment, the buyer will unlock the payment to the seller account. In case of a litigation between the two parties it would be possible to ask the intervention of the ledger's authority which can rule in favour of the seller, unlocking the payment, or in favour of the buyer refunding it.

1.2.10.5 Blockchain as an accounting system

According to the Committee on Terminology of American Institute of Certified Public Accountants (AICPA) Accounting is: "both the science and art of correctly recording in books of accounts all those business transactions that result in the transfer of money or money's worth. It may also be defined as the art of recording mercantile transactions in a regular and systematic manner; the art of keeping accounts in such a manner that a man may ascertain correct result of his business activities at the end of a definite period and also can know the true state of affairs of his/her business and properties by an inspection of his/her books." (Rao, 2012) Accounting is a system who adopted worldwide the double-entry framework, starting from Italy in 1299 and spread by Pacioli in 1494 in all Europe (Smith, 2013), this method is trusted internally but for external purposes it needs the intervention of an external and super-partes auditor to certificate the validity of what has been recorded and auditing is an expensive and time consuming activity. Deloitte in its report "Blockchain Technology: a game changer in accounting" makes the hypothesis a distributed ledger with the property of immutability may drastically reduce the expenditure for external auditing removing the bottleneck. Legit counter argument would be that for this purpose also a centralised universal server would allow the same results as a shared ledger but with fewer costs due to an increase in efficiency. Centralised systems are not fault tolerant, hence the down of the database means the failure of the entire system, hence a certain degree of redundancy is needed; moreover centralization means that the system is susceptible of unilateral manipulations of the data there stored therefore the need of an external auditing control is still needed in order to avoid continuous legal disputes. (Morini, 3/2016).

On the paper “Role of blockchain in accounting and auditing”, which unfortunately is all written in Russian but the abstract, is mentioned the security of records on a distributed ledger capable of resisting to tampering and revision would enhance the strengthened the final results from an accounting stand point because it would drastically reduce the chances of frauds after the data was firstly compiled and uploaded (Melnychenko & Hartinger, 2016).

1.2.10.6 Know Your Customer and Anti Money Loundering

The know your customer or KYC is “The objectives of conventional KYC (Know-your-customer) procedures are the following: making reasonable efforts to determine the true identity and beneficial ownership of accounts; sources of funds, nature of customers' business, the assessment of reasonable account activity, and the identity of the customers' customers” (He & al, 2016). KYC is especially used by bank and insurers for purposes of compliance and anti loundering due diligence. KYC procedures cost, according to Thomson Reuters 60 million dollars per year, plus fines sanctioned to institutes for their misconducts. Parra-Moyano and Ross proposed to implement distributed ledger solutions in order to reduce considerably the cost to manage these procedures. It starts from the description of how KYC is performed currently, basically a sequence of actions that the clients has to do for every bank it want to make business with, mostly sending documents allowing the institution to initiate the verification process. The bank, internally, analyses the client and generate more documents to prove the client has been rejected or accepted on the base of a compliant verification process. Then, after the chapter dedicated to describing the DLT, the authors propose its version of an optimized KYC management based upon a ledger distributed among several financial institutions. The KYC procedure is than done only once by the first bank of the consortium reached by a certain client, successive banks will just have to prove the client contact them to retrieve the file from the shared ledger.

1.2.10.7 Blockchain as a financial market infrastructure

Financial markets infrastructures are defined a paper by Russo and Mooney for the bank of international settlements as “a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions". All this infrastructures have the sole scope, from a very high level perspective, of recording ownerships of assets and clearing contractual agreements for a multitude of different financial instruments. These infrastructures are declined for different purposes in payment systems, central securities depositories (CSDs), securities settlement systems (SSSs), and central counterparties (CCPs), over-the-counter (OTC) derivatives CCPs and trade repositories (TRs):

- Payment systems are infrastructures devoted to facilitate and record the transfer of funds between or among participants. The system is composed by participants and the entities in charge of maintenance. Payment systems may be retail, concentrated to high frequency and small amounts per transaction or be designed for large value transfers. Retail systems may operate both in deferred or real time, using a multilateral deferred net settlement (DNS) or a real-time gross settlement
(RTGS) mechanism, and be controlled by private and public sector. Systems for large value transfers are normally designed for operating in real time and hold by central banks.
- central securities depositories (CSDs), a central securities depository provides securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and redemptions, and plays an important role in helping to ensure the integrity of securities issues (that is, ensure that securities are not accidentally or fraudulently created or destroyed or their details changed). A CSD may maintain the definitive record of legal ownership for a security; in some cases, however, a separate securities registrar will serve this notary function.
- Securities settlement systems (SSSs), a securities settlement system enables securities to be transferred and settled by book entry according to a set of predetermined multilateral rules. Such systems allow transfers of securities free either of payment or against payment. When transfer is against

payment, many systems provide delivery versus payment (DvP), where delivery of the security occurs if and only if payment occurs.

- Central counterparties (CCPs), a central counterparty interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer and thereby ensuring the performance of open contracts.
- Trade repositories (TRs), a trade repository is an entity that maintains a centralised electronic record (database) of transaction data. A well-designed TR that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse (Russo & Mooney, 2012).

In the same contribution Russo and Mooney reported also a wide declination of many if not most of the risk such infrastructures are exposed to:

- Systemic risk arise when the dependency of a large number of different financial contracts is mutual and serialized, meaning that if one contract default the others are effected in some way. This dependency can be fatal also in case of a default of the financial market infrastructure itself if a counterpart is unable to process its contract it may affect many other ending in an escalation.
- Legal risk may arise in case of an unexpected application of the law that may result into a loss. Even if at the end of a litigation, it can still be possible to suffer losses.
- Credit risk involve a counterparty unable or unwilling to correspond its financial obligation.
- Liquidity risk, as we already mentioned, is the adverse possibility of not be able to liquidate a certain position in a relatively short time without having to strongly discount the price.
- General business risk is the risk linked to the financial market infrastructure as a company itself.

- Custody and investment risk, the first one is the risk related to the possibility the custodian actually loose the assets, insolvency, negligence, fraud, poor administration or inadequate bookkeeping. Investment risk arise when the financial market infrastructure invests its own or its participants' resources, such as collateral.
- Operational risk is generated from a failure in the actual physical infrastructure. These operational failures may lead to consequent delays, losses, liquidity problems, and in some cases systemic risks.

The possibilities of Distributed ledgers technology for financial market infrastructures was widely supported by the majority of the papers issued in response of the ESMA discussion paper. The response of the European Central Securities Depositories Association (ECSDA) was extremely positive regarding the future use of such technologies. In the final report of the ESMA which summarized all the positions presented for its call for discussion (ESMA, The Distributed Ledger Technology Applied to Securities Markets, 2017) it has been remarked and confirmed its initial opinion that DLTs will bring many benefits to securities markets thanks to more efficient and seamless processes especially in all the post-trading processes which deal with harmonization of assets exchanged on different infrastructures allowing the definitive record of ownership movements from the standard T+2 to nearly instantaneous.

The ESMA report also of significant potential improvements from the operational stand point with a major reinforcement of system resiliency towards failures thanks to the redundancy of the information stored in many memories across the network.

The possibilities of having automatized contractual covenants management reduces the counterparty risks and real time collateral management with an improvement of market liquidity due to the instantaneous availability of assets after the regulation of contracts.

Overall ESMA expects an important reduction of costs due to economies of scales, disintermediation of custodians, clearing houses and all the intermediaries involved in the post-trading processes, and network effects.

Of course, such an evolution of the infrastructure requires a strict control over risks and challenges associated with that. ESMA posed the attention over the necessity of such a system to achieve said network's size to benefit of the economies of it, not an easy task since it means every actor must come to a common standard, which can take years in particular if the horizon is international therefore interjurisdictional. Is not impossible that in the beginning there will be a great number of different networks that will, eventually combine themselves reducing the numerosity while triggering network externalities. Another key aspect to take into serious consideration is the absolute lack of flawed design, in particular, the paper refers to the DAO hack, which was due bad software architecture. Future governance of such a system is another aspect full of concern and ESMA remark vehemently how important is to integrate a strong governance infrastructure to run all the operations since the early days of a future transition.

1.2.10.8 Trade Finance and supply chain management

Investopedia.com define "Trade Finance" as "the process of financing certain activities related to commerce and international trade. Trade finance includes such activities as lending, issuing letters of credit, factoring, export credit and insurance. Companies involved with trade finance include importers and exporters, banks and financiers, insurers and export credit agencies, and other service providers" (Investopedia, 2016).

Based upon several variables, contractual power, familiarity among the counterparties, rating and prestige, there can be an advanced payment, the buyer pays before receiving the goods or in open account, the goods are first shipped and the payment happens at the collection or even after that moment. These two methods of payment shift the risks connected to the transaction from one party to another (Niepmann & Schmidt-Eisenlohr, 2015). Trade, and international one on a more elevate extent, is effected by a wide range of different risks such as (Lehmann & al, 08/2013):

- Credit risk: The seller usually suffers this risk since implies the possibility the counterparty fails paying its due.
- Transport risk: Every kind of issues that may occur during the shipment of the goods, theft or damaging.
- Risk of fraud: when one of the parties involved is not in "bona fede" and deliberately takes advantage of the other.
- Risk of non-performance: When the client refuses to pay repudiating the contract, this usually leads to legal litigation with costs for both sides

These risks concerns both national and international transactions. The following additional issues may arise in an international trade context.

- Country risk: Concerns all the threats, coming from action that a government may decide to do, that can damage your commerce. This may concern both the importer as well as the exporter. This risk is usually connected with political instability and may lead to default of payments, requisition of properties and so forth.
- Legal risk: Difference in legislation in overseas countries that might have impact on import procedures, taxations, property rights and other related subjects.
- Currency risk: The fluctuation of exchange rates may erase seller's profits or increase buyer's costs. This risk has a double side because it is a zero sum game, hence if a party suffers the other one gains.

Bank intermediated trade finance is the most common way corporations use to finance their supply-chain and to mitigate some of the risks I cited before, especially what is connected with the counterpart and the country. Using several financial instruments, it is possible to improve liquidity, facilitates payments and improve data visibility Fig[37].

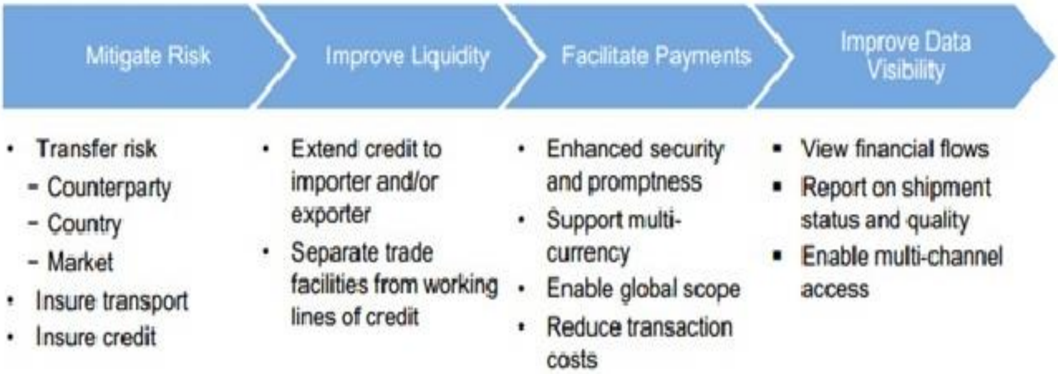


Figure 37 Four elements of Trade Finance (Manju, 2016)

Through trade banks, banks or business units that provides services for export/import purposes, companies are able to use several financial instruments to facilitate their commerce (Swedbank, 2016):

- Letters of credit Fig [38] are banks guarantees that, in case of inability of the buyer to fulfil the payment, it will cover the amount mandatorily. Typically, banks require some collateral as an insurance against the default of the buyer and a percentage of the overall payment as a fee for its service. Letters of credit are not revocable unless the seller gives its consent. A letter of credit may be "commercial", which the issuing bank makes a payment to the beneficiary, or a "stand by" one, which requires a payment from the bank only in the case of default by the buyer. Letters of credit may involve more than one bank when another one back the first, in this case the letter of credit is said "confirmed". Letter of credits are also used by exporting companies as a mean for factoring their credits we reselling them on a very liquid secondary market, this is allowed by the issuing bank that makes the letter "transferable" (Investopedia, Letter Of Credit, 2016).
- Guarantees Fig. [38] are used to cover the risk of noncompliance by one of the involved party, one common instance is the failed delivery of the good or the missed payment. In case of no completion of some contractual agreement, the party offended may ask the guarantee for a

certain amount as compensation, and then the financial institute that vouched may ask for repayment to the faulty party. Guarantee agreements are fairly similar to L/C but they offer stronger protection since it can be extended also to cases of non performances, while the first usually are limited to missed payments only (UNECE, 2017).

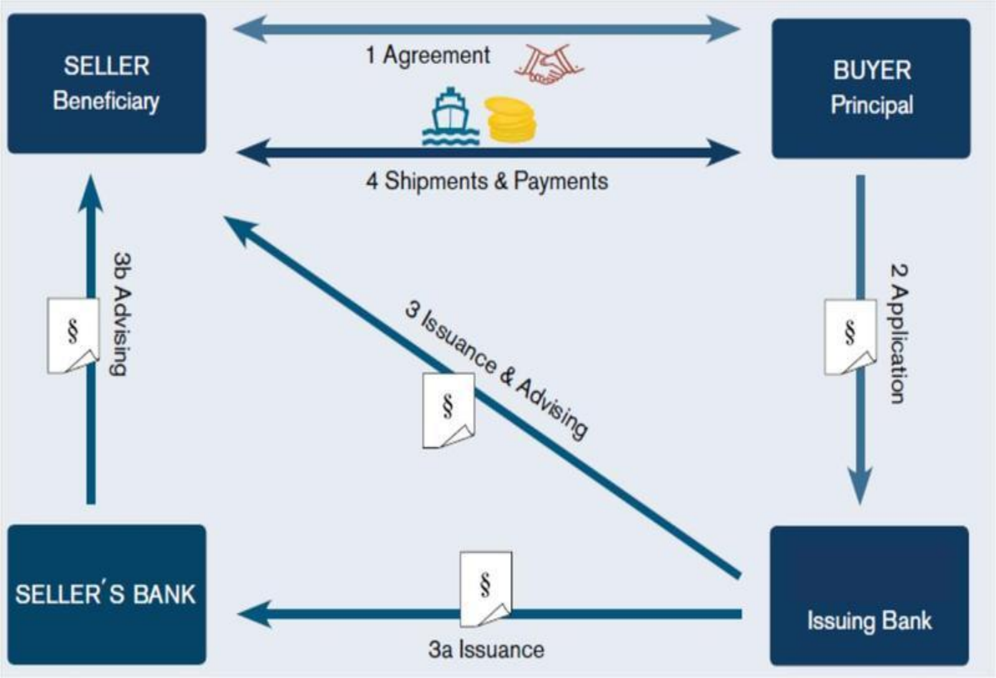


Figure 38 Flowchart for Letters of credit and Guarantees (UNECE, 2017)

- Documentary collections are agreements that sees a remittance bank entrusted with the collection of the payment by the seller. The bank receives from the sender the needed documents for the buyer to claim the goods delivered to some warehouse, without those it would be impossible to retrieve the shipments. The buyer has to pay to the bank the due amount, only after that it receives the documents for collecting the goods. This instrument prevent the buyer from stealing the goods but in the meantime it still exposes the seller to credit risk since it can still be that it will not received what is due. In such a case the seller will have to deliver the shipment back to its warehouse or try to sell it on loco, presumably, at discount (UNECE, 2017).

From the descriptions above the reader should be able to see the opportunity for a system based upon a tamper proof distributed ledger. The Euro Banking association’s opinion tends the same way. In their paper about the potentialities of crypto technologies within trading finance they presents several use cases such as the exchange of reliable information and the reduction of lags due to ownership changes. The irrevocability of a commitment published on a proper distributed ledger cover the parties from the risk of seeing their protection retract arbitrarily and the signature of the contract made with the public key vanish all the possibilities of frauds through the forgery of the document. The key aspect of Bitcoin is the nearly instantaneity of cross border payments which is intuitively a significant improvement for international trade. Banks and corporates may benefit from such an infrastructure.

A paper by the European Banking Association (Szmukler, 2016) states distributed ledger technologies will be able to address many issues relate to trade financing thanks to the “real time transparency” of the information of every transaction, payment details, transfer of ownership and other underlying variables. The immutability of the information stored on the Blockchain would make litigations much less time consuming because of the certainty that what was written, signed with the respective private key and time stamped thanks to the blocks’ order is the absolute truth. On the Bitcoin’s Blockchain, it would be possible, for example, to issue a transaction hashing the content of a contract within it. In case of litigation the copy of the contract held for true would be the one that hashed give the same result as the one stored upon the chain. The possibility to create automatized contract capable, for instance, to pay the due amount as soon as a transaction is issued to the network where the receiver of a shipment sign with a public key in order to obtain the cargo would permit the implementation of automatized customs where only few authorised can enter.

This innovation would increase the safety especially in those countries where theft is particularly common. In order to avoid every type of bottleneck it would be better to have every actor involved on the distributed ledger as in Fig.[]. The presence of a document such as letter of credits or of smart contracts shaped as escrows able to be triggered by a public third party such as the custom, would improve both the reliance of the authenticity of the document and the probability to be paid as agreed. In addition, a system of interconnected ledgers allows the immediate liquidation of a letter of credit by reselling to investors, monetising it before its due date.

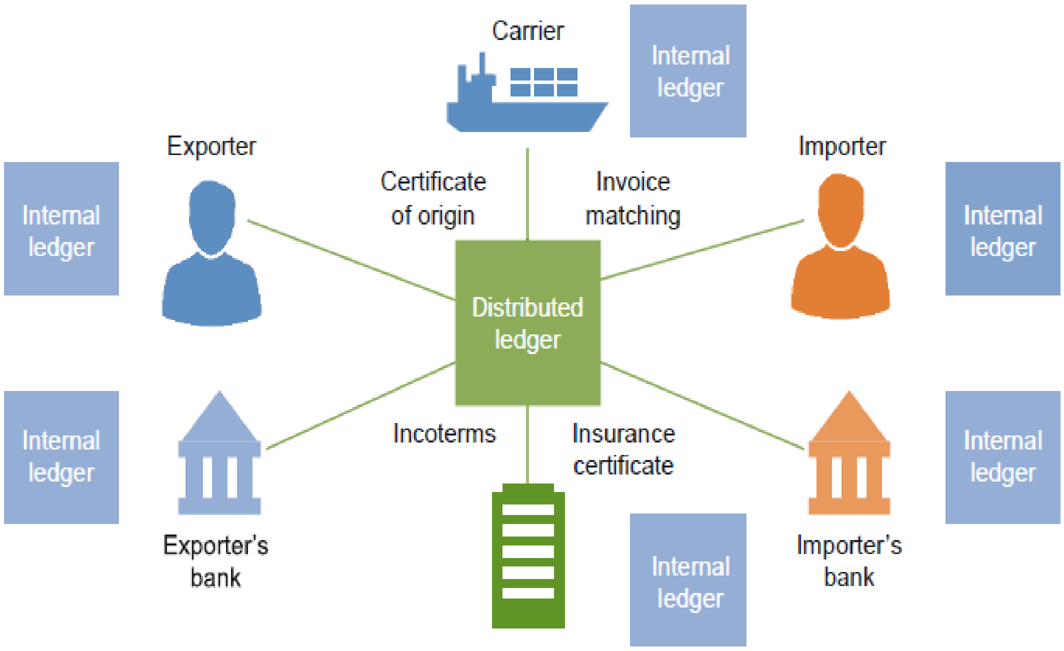


Figure 39 Using distributed ledgers in trade transactions (Szmukler, 2016)

2 Scenario Planning: Methodology and Results

The precedent literature review aimed firstly to understand the industry of crowdfunding in all its different denominations and peculiarities. Of course being a thesis with the claim to improve the actual framework the focus was latter moved upon the issues and open questions of the topic. Summarizing the study highlighted how major concern behind the industry is linked with the shadow of uncertainty that envelopes it. Said uncertainty shows itself in the valuation of the backed venture, from the actual merit of its proposition to the capability and honesty of the team behind it. Apart from aspects linked with the enterprise itself uncertainty is also fed by the highly difficulty for an investor, in case of need, to dismiss its position without suffering heavy losses or long waits, this is of course due to the illiquidity of those securities and to the very high transaction costs necessary to find willing buyers.

With the experience of the DAO campaign, this review had the logic and narrative link to move to towards to the next part of the literature concentrated on Distributed ledger technologies and addressed from a multidisciplinary standpoint, in order to fully comprehend the possibilities of this technological breakthrough and its impediments. We understood how the protocol for the distributed consensus shapes all the properties of a network and hence the regulation and utility of each different option.

The next step is the actual original contribution of this entire work of mine to the academic literature and perhaps to the crowdfunding industry. For this purpose, this work will use the tool of Scenario Planning, defined by Schoemaker as "a disciplined method for imagining possible futures that companies have applied to a great range of issues. […] Scenario planning simplifies the avalanche of data into a limited number of possible states". Godet defined a scenario as the description of a future situation with the narration of the curse of events that leads to that ending. Also the there are two typologies of scenarios, one that starts from the past and flowing trends ends to the future state is defined as "exploratory" on the other way round a scenario that starts from a desired or feared outcome and the study is to identify the set of actions to make it possible or to prevent it is called "anticipatory" (Godet, 2004). The choose of this tool is supported by the paper of Torsten Wulf and all in which they stated, "the integration of scenario planning into strategic planning has the potential to lay the foundation for an innovative, integrative concept of strategy creation" (Wulf & al, 2010).

This work of thesis aims of course to see implemented a secondary market for crowd based securities on a distributed ledger, therefore this scenario is going to be "anticipatory". Referring again to Godet the main stages of the scenario creation are the identification of all the key variables, the identification of the actors involved and their roles finally obtaining the path that is more likely to end in the wanted scenario. For Wulf (Wulf & al, 2010), frameworks as if scenario planning there is the need to fulfil four major requirements:

- Multiple options: There is the need to provide as an output a set of different scenarios in order to be able to build strategies in a manner to prevent the unwanted ones while facilitating the best cases.
- Multiple perspectives: Scenarios must take into consideration the presence of multiple stakeholders involved in the project. Multiple interests must converge on the realization of the best outcome. It is also important to take into consideration multiple standpoints to assess the solidity of the assumptions.
- Systematic, tool based process: The process that leads to a scenario must be clear in order to be understood by all the parts involved, and for its own credibility.
- Flexibility: The best scenario must be reached in the most flexible way in order to be always ready to face the unexpected.

The scenario based approach to strategic planning should enable strategy makers to prepare plans for multiple situations while integrating internal and external assumptions and points of view, which are two fundamental aspects of the innovation nurturing. The scenario generation tool this work is going to implement is taken by the work of Wulf and Fig. [40] presents a quick overview.

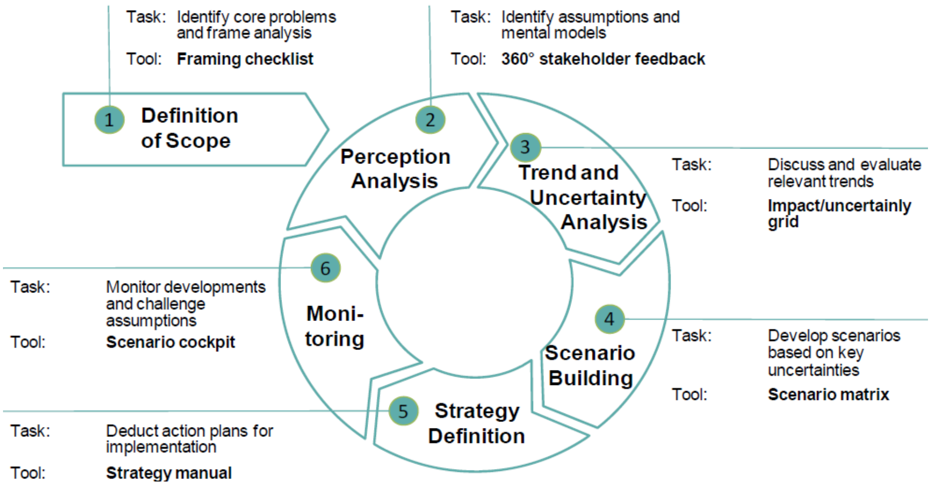
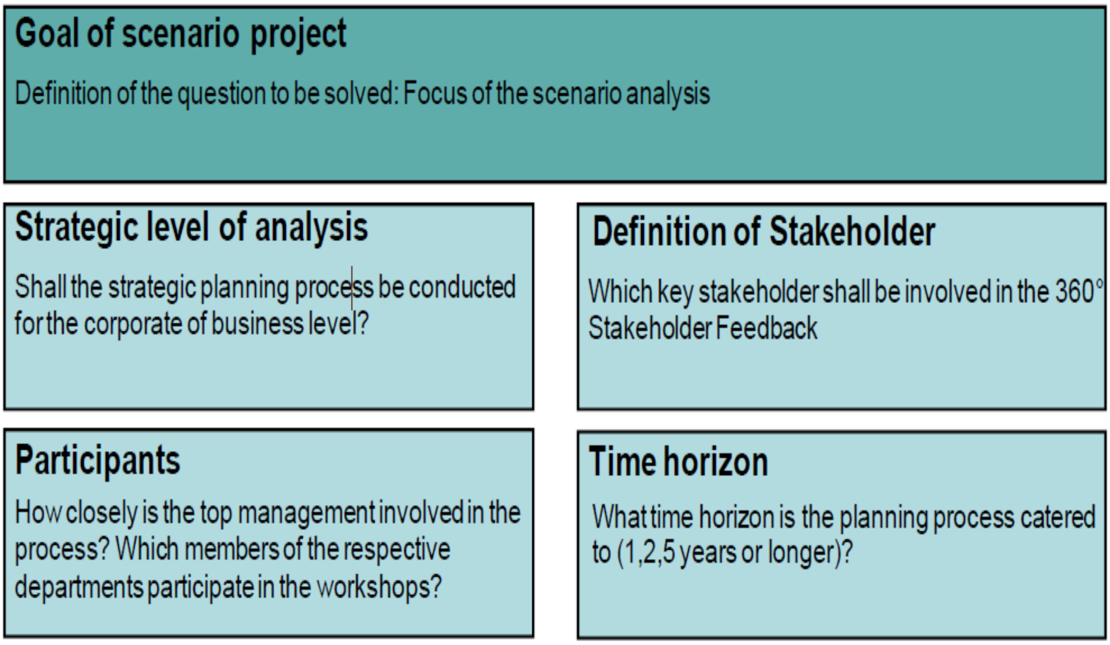

Task: Identify core problems and frame analysis
Tool: Framing checklist
Task: Identify assumptions and mental models
Tool: 360° stakeholder feedback
1 Definition of Scope
2 Perception Analysis
3 Trend and Uncertainty Analysis
Task: Discuss and evaluate relevant trends
Tool: Impact/uncertainly grid
6 Moni-toring
Task: Monitor developments and challenge assumptions
Tool: Scenario cockpit
4 Scenario Building
Task: Develop scenarios based on key uncertainties
Tool: Scenario matrix
5 Strategy Definition
Task: Deduct action plans for implementation
Tool: Strategy manual

Figure 40 Overview of the scenario-based approach to strategic planning (Wulf & al, 2010)

As showed, the model consists of six steps. The definition of the scope has the object to define the overall boundaries of the project. Wulf developed for this purpose the "Framing checklist" Fig. [41].



Goal of scenario project

Definition of the question to be solved: Focus of the scenario analysis

Strategic level of analysis

Shall the strategic planning process be conducted for the corporate of business level?

Definition of Stakeholder

Which key stakeholder shall be involved in the 360° Stakeholder Feedback

Participants

How closely is the top management involved in the process? Which members of the respective departments participate in the workshops?

Time horizon

What time horizon is the planning process catered to (1,2,5 years or longer)?

Figure 41 Framing Checklist

This additional instrument helps the process by posing five questions:

- Goal of scenario project: what issues we are going to tackle with this project?
- Strategic level of analysis: This project is going to address a particular business function? A business unit? An entire company? An entire Industry?
- Definition of stakeholders: Who will be involved into the project? Who has the power and the know how to see it succeed or fail? Their role is going to be active or passive?
- Participants: This question is to define the team that is going to take care of the scenario and strategy planification.
- Time Horizon: The time frame in which the scenario will eventually emerge.

The second step is the perception analysis, during this phase all factors that can influence the future of the scenario are gathered and listed. These factors may be trends or major key source of uncertainty in the industry, with an explanation of how they would be able to influence the outcomes (Schoemaker, 1995). The source of information for this phase is a representative sample of the already mentioned stakeholders for a third party, wide ranged and fully trustworthy information harvesting. The paper presented its own tool in the form of “360° Stakeholder Feedback” Fig. [42]. The stakeholder feedback is the result of a survey that contains both open and closed questions concerning factors that might have an influence on the scenario.

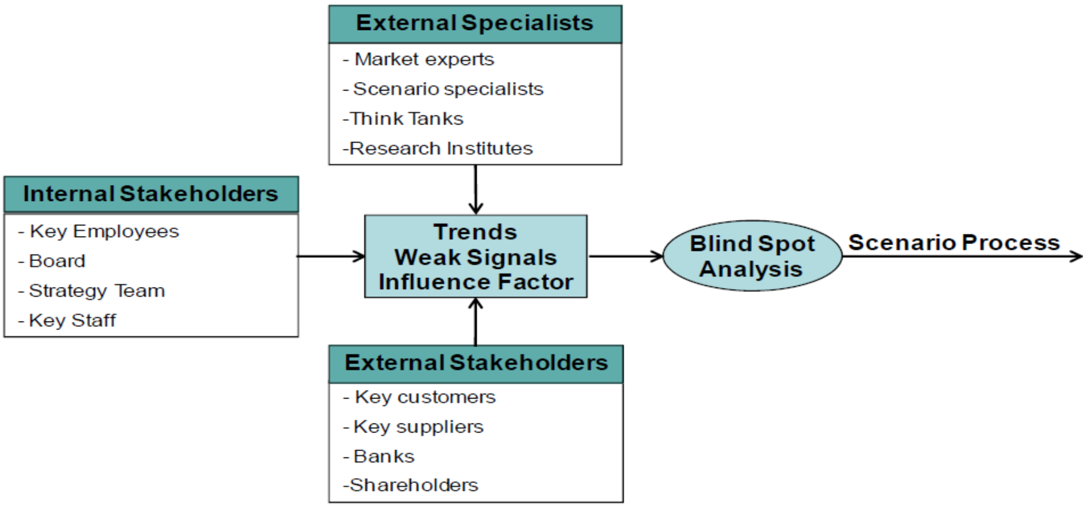


Figure 42 360° Stakeholder Feedback

After having obtained all the feedbacks from the sample interviewed the process may enter in is third phase where trends and uncertainties are analysed and evaluated with respect to their possible force of impact on the project. Again, the author proposed a tool for this task Fig. [43]

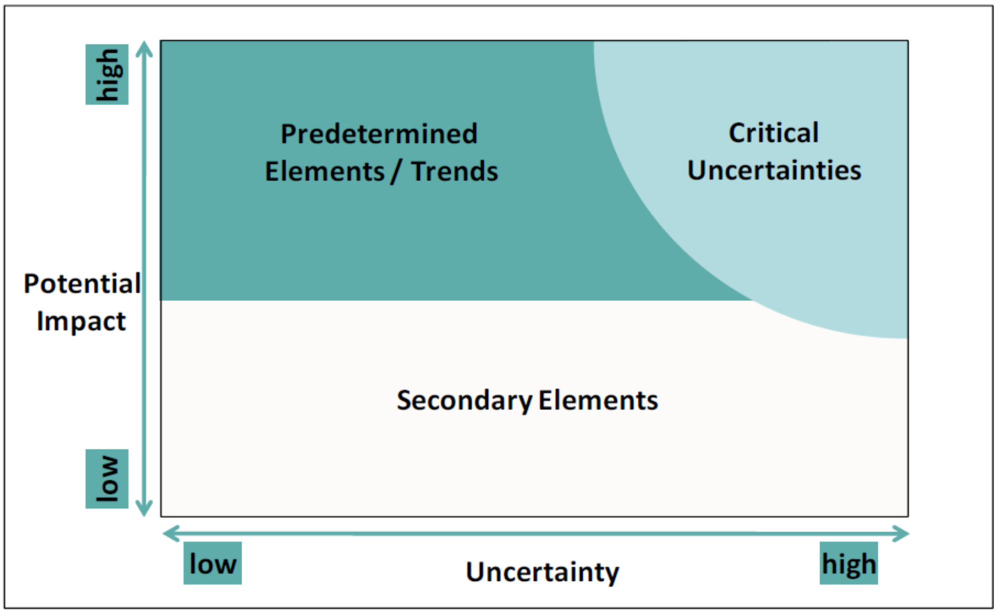


Figure 43 Impact/Uncertainty Grid

Once we have completed the organization of all the factors, the work may proceed towards the fourth stage that is scenario building. Scenarios are direct consequences of the trends and uncertainties depicted previously therefore there can be as many scenarios as many combinations of key factors there are. The tool for the phase four is the scenario matrix, in Fig. [44] presented with the combination of two factors, therefore a 2-D diagram.

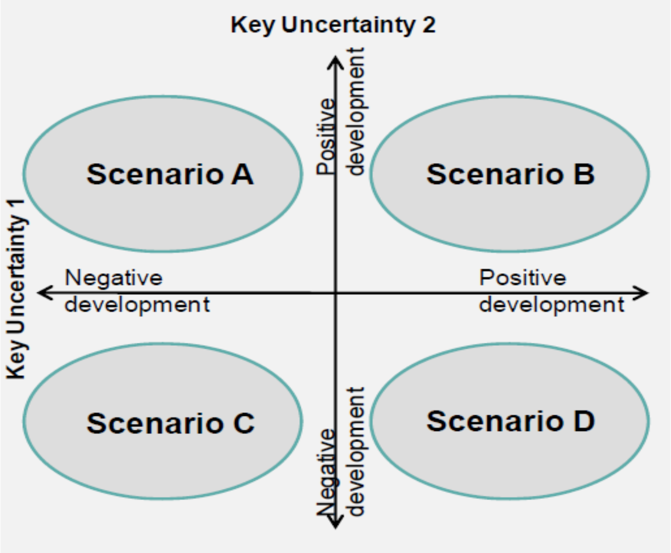


Figure 44 Scenario Matrix

After having produced all the scenarios desired it is necessary to go deeper describing in copious details regarding how different variables have influenced the history managing to reach that outcome. This approach is based upon causes effects relations, for this scope the instrument suggested is the "influence diagram". This phase is extremely useful to assess the consistency and plausibility of what has come in the end. This may lead to consider some scenario as paradoxical, hence not taken into further consideration. The strategy definition aims to size the actions that would benefit the most to the realization of desired scenarios, while preventing negative ones. Finally, once the best course of action is finally sorted out it is necessary to implement a structure of key performance indicators capable to monitor the state of the work during the project lifetime.

2.1 Goal of scenario project

The goal of this project is to asses if future scenarios are going to be favourable for the introduction of a crowdfunding market infrastructure based upon blockchain.

For this matter, we must analyse the future scenarios for the securities based crowdfunding to understand if it is worth in the first place. In this regard, this work is interested about the strength of the crowdfunding trend in terms of volumes raised and number of players, platforms, campaigns and investors. Among these scenarios, it is important to understand whether is possible the effective implementation of a financial infrastructure based upon the blockchain, the possible impediments, challenges and drawbacks.

2.2 Definition of the Scope

This work started with an extended research into security based crowdfunding in order to understand one after another what are the main issues that could prevent or at least strongly delay the full maturation of this financial instrument. Through this research, several possible areas of intervention came to the attention of this work, mainly related with information about the future and about how it is spread across different stakeholders. We had the uncertainty about the real value of said assets, for equity the real value of future cash flows in dividends, while for debt whether or not the backed firm will be able to repay what is due. We had uncertainty also for who decides to buy crowd based securities, if after a certain period of time it is going to need quick liquidity for a new investment or for its own personal motifs how is going to sell the position without significant losses because of transaction costs and illiquidity of it? How the crowd is going to control the well behaviour of the management team after it received the seek capital?

To these questions, this work proposed a solution would come from the implementation of a fluid secondary market. The presence of an active secondary market for equity and debt may allow investors to better decide whether or not back the firm in case of another round of capital raising, also it can help future issuer to better price their assets using methods similar to what is commonly implemented in stocks markets like multiples. The possible realization of such a structure can be prevented by the small size of the free float and the low values of the offers. These two aspects would have stop any kind of traditional trading infrastructure but, perhaps, not one based upon the new distributed ledger paradigm that since Bitcoin has gone in massive hype.

From this standpoint the scope of this work is to understand if the presence of a secondary market can overcome those issues and if a Distributed Ledger network may be a viable solution for crowd based security trading.

2.3 Definition of stakeholders

Stakeholders from this project are experts both from the DLT field and of course from the crowdfunding one. The internal perspective is filled by the experts from the crowdfunding environment since they are the ones in charge to receipt the innovation of secondary market and distributed ledgers, also they are the one who should federate creating a consortium where clients logged on a platform may be able to trade securities issued on all the other platforms stored on the ledger. The external point of view is represented by experts and evangelists of Blockchain and Distributed ledgers, their aim is to support or disprove the applicability of such solution for the problem in question.

In Tab. [] experts interviewed are reported alongside their company of affiliation and there area of expertise.

Expert	Area of Expertise	Company
Alessandro Saglimbeni	Blockchain	Blockchainlab
Marco Monaco	Blockchain	PWC
Giorgio Mazzoli	Legal-Blockchain	Coinlex
Tommaso Baldissera	Equity Crowdfunding	Crowdfundme
Dave Freedman	Crowdfunding	Freelance Journalist
Antonio Lafiosca	P2PLending	Borsadelcredito
Matteo Masserdotti	Equity Crowdfunding	TipVentures
Matteo Tarroni	Invoice trading	Workinvoice
Ettore Decio	Invoice trading	Workinvoice
Thomas Bertani	Blockchain	Oraclize

Table 9 List of interviewed experts

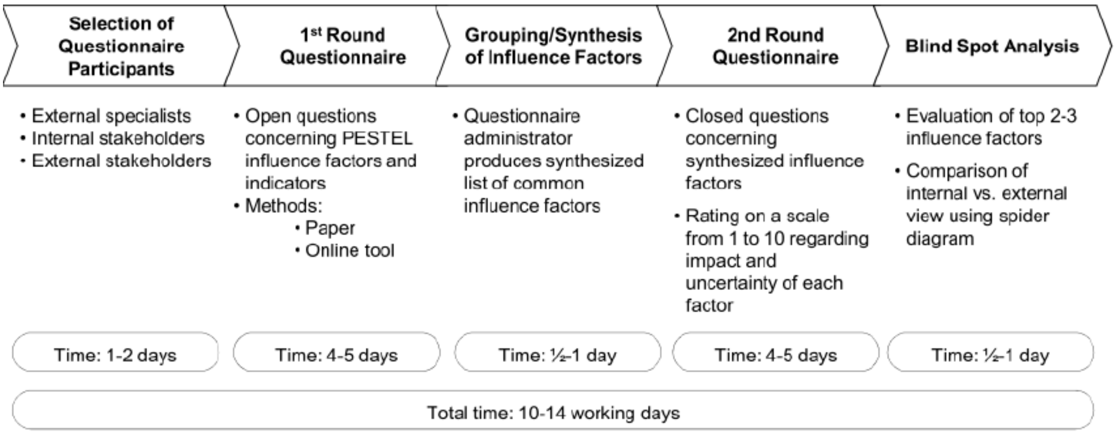
2.4 Level of analysis and Time horizon

The level of analysis of this scenario planning will not be limited to a single platform but to the whole industry, also because this kind of solution does not come without the participation of a minimum number of different players for obvious motifs. Time horizon is not concerned in this work.

2.5 Tool description-360° Stakeholder feedback

The 360° stakeholder feedback gathers and manage all the signals, strong as well as weak, and allows the identification of blind spots establishing a comprehensive list of factors that potentially can influence the future outcome of the desired scenario, according to their potential force of impact and enabling conditions.

The instrument is the result of a two steps survey process as depicted in Fig. [45]



Selection of Questionnaire Participants	1st Round Questionnaire	Grouping/Synthesis of Influence Factors	2nd Round Questionnaire	Blind Spot Analysis
• External specialists • Internal stakeholders • External stakeholders	• Open questions concerning PESTEL influence factors and indicators • Methods: • Paper • Online tool	• Questionnaire administrator produces synthesized list of common influence factors	• Closed questions concerning synthesized influence factors • Rating on a scale from 1 to 10 regarding impact and uncertainty of each factor	• Evaluation of top 2-3 influence factors • Comparison of internal vs. external view using spider diagram
Time: 1-2 days	Time: 4-5 days	Time: ½-1 day	Time: 4-5 days	Time: ½-1 day

Total time: 10-14 working days

Figure 45 360° Stakeholder Feedback Process

In the first round is asked to the sample to answer to open questions concerning influence factors and what kind of already existing instruments or KPI may size such information. It is advised to devise the questionnaire following the ratio of a PESTEL analysis, in order to consider every possible source of influencers. The feedback from this first round is then analysed and synthesized into a new questionnaire, this time with closed answers, like strongly agree or from 1 to 10. Of course, a strong success factor for this instrument is the composition of the sample, heterogeneous but still consistent with the context and as wider as possible. Once received the result the search for blind spots, what it has been highlighted by external stakeholders but not by internal ones and visualized on a tool such as a spider diagram. This last part concludes the 360° stakeholder feedback the result are the blind spots between the internal stand point and the external whose developments will be taken into consideration for the generation of future scenarios and courses of action.

The first part of the 360° stakeholder feedback will be completed not with a survey but thanks to the literature review in order to have a wider and international point of view that, just limiting the analysis to national experts, it could be missed. Nevertheless, the result of this preliminary part will be presented to said experts alongside with the survey.

2.6 P.E.S.T. Analysis

In this sub-chapter will be presented all the different sources of possible friction for the implementation of such an infrastructure. The instrument is going to be used is called the Political, Economic, Social and Technological analysis or PEST. This instrument has been used since the sixties and boomed in the eighties with researchers like Fahey, Narayanan, Morrison, Renfro, Boucher, Mecca and Porter and it is useful to show in a systematic manner all the different trends capable to influence for the good or for the bad a certain venture.

- Political factors: Adverse tax policies against the capital raised during a campaign may be a real threat for the flourishing of this industry. On the other hand tax relief for financial gaining coming from crowd based securities, hence the investors benefits from a lower tax rate, can be a significant incentive towards the adoption of such an option. The recognition of the distributed share as a legal document proving the ownerships of the assets stored on it is of paramount importance for the enforcement of the rights coming from the investments in assets like debt or commercial credits. The legal restriction of crowdfunding is another critical eventuality to be taken into account, in the literature it has been seen how there are restrictions about the maximum amount realisable during a single campaign that can make it economically not advantageous. Finally, the international aspiration of a consortium can be significantly interfered by different regulations. Increase in transparency of issuing companies should call for more equity offerings under legislations such as the title II of the Jumpstart Our Business Start-ups (JOBS Act).

- Economic factors: Definitely one major factor for the growth of crowdfunding is the impossibility for innovative start-ups and SMESs to obtain banks loans because of the aftermath of the 2008 and 2011 financial crisis that generate a massive credit crunch towards highly risky ventures. Current central banks policies of low interest rates makes investors eager to find new sources of high return for their portfolios. Growing interest of institutional investors such as business angels and venture capitalists. Future economies of scale and economies of network coming from consortia built around shared ledger platforms also the improvement of practice in planning and implementing this kind of solution would, eventually, lower the costs associated to such investment.
- Social: Generations such as millennials and digital natives will be more prone to invest online, the peer to peer lending will be seen as more sustainable than investing through the traditional financial system as a report from Goldman Sachs says "Millennials are more likely than any other generation to donate to organizations online and via mobile; further, campaigns on donations platform such as GoFundMe could be more specific and provide more transparency in how the money is being used vs. donating to large, established organizations where there could be trust issues. Additionally, rewards based platforms like Kickstarter appeal to Millennials by allowing backers to fund films, music, and games and connect with the creator in an authentic or artisanal way. The implied level of ownership or patronage implied is also appealing to millennial funders" (Terry & al., 2015). A wider number of investors will be beneficial for the "wisdom of the crowd" and for the overcome of information asymmetries.

Populists’ movements, deeply antagonists of legacy institutions such as big banks and also governments, depending on their political allegation, can provide a solid base for both campaigners and investors. The growth of open source and free software innovation can enhance the apparition of new business idea, hence more start-ups calling for initial capitals through crowdfunding.

- Technological: The level of security of personal information is perhaps the most concerning aspect of the whole project, investors or any other kind of user wants to be certain its privacy is guarantee by the highest standards possible. Another fundamental factor is the overcome of issues concerning scalability of distributed ledgers. New consensus protocol able to provide the same specifics of a proof of work without the waste of energy. The Fintech trend will be of extreme importance for both distributed ledgers technologies and crowdfunding because they are major declinations of it in the first place. The presence of new entrance with new innovative financial service may make trans-economies of scope arise allowing cooperation among different service sharing the same ledgers. Projects like R3’s Corda and Hyperledger’s Fabric are essential because, being open source allow scientific and technological transfer for applications based upon the same solutions but with no mean able to reach the level of investments needed.

2.7 Feedbacks

After having gathered all these success variables this work produced and sent to several experts and active actors in the industry a questionnaire and asked for interviews to assess their position about the strength of said variables and their impact on the future scenario. The author also had the opportunity to personally interview some of them. Results from the questionnaire reserved to experts and professionals where used to place the variables within the Uncertainty and Impact graph.

In order to answer to the question whether an easy system for trading crowd based securities would have enhanced the industry, I exploited the occasion provided me by the interviews to pose this query directly to involved experts. All the questioned experts agreed upon the possible growth of the industry if such feature were available. In addition they posed the possible effect in a range from an increase of 50% to more than doubling the actual market.

2.7.1 Future growth of crowdinvesting

Worldwide crowdinvesting is receiving great stimulus and its growth is solid and steady. Respondents are not entirely confident Italian crowdinvesting industry would be able to keep the pace, in fact, they believe it is already quite lagging if compared to other countries. Mr.Masserdotti from TipVentures related this lateness to two main factors, which were already highlighted by the P.E.S.T analysis, the government's and the VCs' interest. This is limited to Italy since they acknowledged the, mentioned before, growth of the industry in other countries.

2.7.2 Role of Public Authorities and Regulators

From both questionnaires and from direct feedbacks it has been pointed out taxation could play a critical part in the future of crowdinvesting because they would increase considerably the expected return of an investment, if it were profitable of course. In Italy there are already fiscal exemptions concerning investments in crowdfunding ex-Legge di Stabilità 2017, other exemptions were presented within the plane "Industry 4.0". Interviewer were not certain about the possibilities in the foreseeable future of new aid from the fiscal standpoint but they were confident what has been given until now will not be revoked. During an interview it was also been explained how, for a "secondary" trade, it is needed the presence of a third party entitled by the authority to oversee the transaction. The interviewed stated how this incumbency is of extreme uncomfortability for both parties because they have to proceed "off line" and they have to pay for the notary agent, increasing the illiquidity and the inefficiencies of the already quite inefficient secondary market. After the explanation of what a distributed ledger network is the interviewed stated it would be of significant benefit for the crowdfunding industry.

In the same way as for taxes, public intervention on the industry is seen as a major source of potential stress to the industry. The common fear is the regulator, in order to give more protection towards, investors may pose more barriers for them to access the service. In particular, they fear in the future thresholds in terms of maximum commitment or maximum realisable capital per campaign, presented in the literature review, may be lowered. Another concern for platforms comes from the fear to be asked in the future to fulfil more bureaucratic incumbencies making more difficult for platform to operate their business. On the other and a relief from these kind of threats would help greatly the sector. Overall, there is a great deal of uncertainty above anything related with public authorities.

2.7.3 The growing interest of institutional investors

Another trend that found most of the interviewed aligned toward the same opinion is growing interest of institutional investors specialised in early stage financing, business angels and venture capitalists for instance, will influence greatly on the development of crowdinvesting and they believe this momentum is quite certainly going to continue in the next future. The motifs behind the high impact factor of this trend are mostly linked with the overcome of information asymmetries thanks to the possibilities of institutions prepared to check thoroughly start-ups and other non-listed companies. By investing into a campaign, institutional firms send to the market positive signals about the real value of it, especially from the managerial and operational standpoint, while the crowd send to them signals about the possible market reception of the business proposition. For this reason, the two are not in complete trade off one with another but it has been noticed how low boundaries in the total maximum realizable amount would depress the action of institutional investors. A possible solution suggested would be to link the cap of a certain campaign with the level of potential commitment of institutional investors, for instance a campaign that doesn’t receive any attention by sophisticated investors would maintain the lowest cap while another that receive x% from a business angels can be entitled to raise the boundary. Mr. David Freedman, Co-author of “A Brief History of Crowdfunding”, does not agree on the potential impact of institutional investors because: “most crowdfunding investors will tend to be unsophisticated (non-accredited), inexperienced, and local -- maybe more interested in community development and support for friends than return on investment. Eventually institutional and sophisticated investors will gravitate to Regulation D Rule 506(b) which is not crowdfunding (because it prohibits general solicitation)”.

2.7.4 Recognition of Distributed Ledger Technologies as reliable notary systems by Public Authorities

For this critical success factor, the author asked the opinion from a lawyer extremely active in the Italian Bitcoin and Blockchain community, Giorgio Maria Mazzoli, main contributor of Coinlex, a blog specialised in jurisdiction of cryptocurrencies. Mr.Mazzoli firstly answered redirecting the author’s attention towards the art. 2704 codice civile: “La data della scrittura privata della quale non è autenticata la sottoscrizione [2703] non è certa [2787, 3] e computabile riguardo ai terzi, se non dal giorno in cui la scrittura è stata registrata o dal giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici [2699] o, infine, dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento (1). La data della scrittura privata che contiene dichiarazioni unilaterali non destinate a persona determinata [1992] può essere accertata con qualsiasi mezzo di prova. Per l'accertamento della data nelle quietanze il giudice, tenuto conto delle circostanze, può ammettere qualsiasi mezzo di prova [1195, 1199] (2)”. Mr. Mazzoli highlighted “"La data della scrittura privata della quale non è autenticata la sottoscrizione non è certa e computabile riguardo ai terzi, se non dal giorno in cui... si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento", which means that in the absence of an authentication by a solicitor of the time and the content of a document, it is possible to provide other means to recover said information, hence, concludes Mr. Mazzoli, the proof of existence of a timestamped document hashed on a blockchain or on a distributed ledger. Mr.Mazzoli argued that, despite the absence yet of real cases in which the authenticity of documents where provided by distributed mathematical timestamping, some countries have already explicitly recognised the value and the legitimacy of such a notary system. For example Arizona (Higgins, 2017) and Vermont (Erly, 2017). Mr.Mazzoli concludes the legal aspect is going to have a massive impact but the innovation machine is already started and it is not a matter of ifs but only when.

2.7.5 Role of financial crisis and credit crunches

The financial crisis in the United State and the sovereign debt crisis in the Eurozone are seen as major triggers for the blooming of crowdinvesting, this is renowned by literature and has been acknowledge by interviewed as well with an unanimous consensus. The sensation of experts, concerning the possibility the current situation will go on in the foreseeable future, is that crowd industry will "benefit" from the condition of lack of traditional sources of capitals, maintaining momentum for further growth. The hunger for higher returns because of low interest rates is not seen, on the other hand, as a particularly impactful variable, by the opinion of questioned experts.

2.7.6 Impact of generational shift and social evolution

Feedbacks from experts agree on giving a low impact factor on millennials and digital natives starting earning, hence investing. The main reasons for this lack of confidence is due to the lack of resources younger generations are going to experience because of the macroeconomic scenario that is characterized by lower wages and higher flexibility of work and to the future low investment proficiency of these two generations. This last note is particular important if we consider that many legislations on the matter link the admissible amount with the knowledge of the investor, hence willing investors would be forced to limit their exposure because of illiteracy on the subject. Another question concerned the anti systemic sentiment that boomed soon after the great financial crisis and generated many movements within a wide range of different context, from the political to the social and, of course, including the financial one. Experts expressed strong convincement that such tendency is strongly positive for crowdinvesting, since allows direct wealth management without having to rely upon legacy financial institutions and it is perceived like a way to help start-ups and SMEs without fearing to subsidies large corporations. Strongly related to this matter the open source and free software movement allows start-ups to free ride a level of research and development impossible to achieve elsewhere creating new opportunities for them to develop new business proposal to be exposed in crowdfunding campaigns.

2.7.7 *Evolution of Distributed Ledger Technologies*

Many of the issues concerning the technological and operational evolution of distributed ledger networks are subject of copious interest by the open source movement and by many institutional investors. This led the interviewed person to believe the technological overcoming is not a source of great uncertainty, on this matter the major one is the regulator’s approach towards its implementation. Mr. Masserdotti argued about the lack of people actually able to build such systems, that are not “already millionaires of their own”.

2.7.8 The growth of Fintech

The possible role of fintech evolution on the crowdinvesting was perceived not in a unanimous way. The feedbacks from the survey reported both very high impact factors as well as minimal ones. The author asked Mr. Freedman why did he think Fintech evolution has no impact on crowdinvesting and his answer was that fintech involves so many areas that it is impossible to relate their growths. On the other hands, other interviewed believes Fintech offers green fields for new start-ups that can seek early seeds by crowdinvesting. In addition, fintech branches such as APIs have believed to increase the usability of crowdfunding services without using other prohibitively expensive services, such as robot advisor able to include assets from the crowdinvesting industry within some returns seeking portfolios.

2.8 Scenarios Generation

With the results obtained with feedbacks provided by surveys and interviews it is now possible to determine if a certain variable is actually given as mostly certain for the future or whether it is still covered by a great deal of uncertainty, also to divide the highly impactful factors from the ones of secondary importance. As explained in the introduction of scenario planning this part needs to be done properly because critical uncertainties are responsible for the generation of different possible future contexts. This work is going to consider two major sources of uncertainty, one concerning crowdinvesting the other distributed ledger technologies. It appears quite clearly one critically important source of uncertainty comes from the public authority. Interviewed experts were not able to read whether the direction of the regulator's mind tends towards increasing the "protection" for investors by making more difficult for them to commit money or, on the contrary, if it is going to provide the industry with more momentum by deregulating it or increasing taxes benefits for capital gains or losses. From the distributed ledger standpoint, again the regulator presents the main source of uncertainty. In this particular case the motifs of concern came from the capability of a network of crowdfunding to adopt the proper solutions to guarantee the maximum level of security for itself and privacy for the end user while be able to maintain fully transparency for the authorities to prevent frauds, money laundry or tax evasion. In Fig.[46] four different scenarios have been plotted.

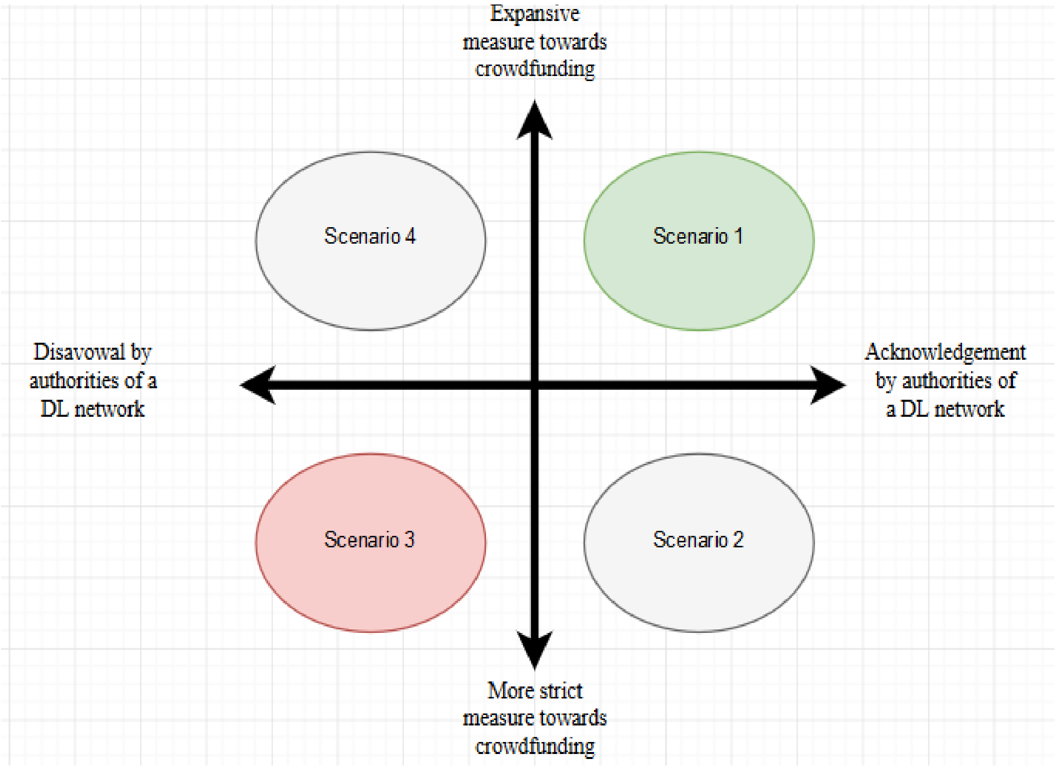

Expansive measure towards crowdfunding
Scenario 4
Scenario 1
Disavowal by authorities of a DL network
Acknowledgement by authorities of a DL network
Scenario 3
Scenario 2
More strict measure towards crowdfunding

Figure 46 Scenarios Diagram

Scenario 1 is, of course, what this work consider to be the best eventuality possible since it would benefit by a conveniently positive attitude from the regulator both regarding the crowdinvesting industry as well as towards the proposed solution for a secondary market. The worst scenario, on the other hand, would not allow any kind of implementation of blockchain as a financial infrastructure and would make the industry suffer greatly due to the increase of the difficulty for entrepreneurs to apply for a campaign ad for investors to commit the amount of their choosing. In case of scenario 2 it would be still possible to implement a solution, as the one this work is studying, but it would not be economically profitable since the entire industry would be crippled destroying the primary market, hence not allowing the creation of a need for a secondary in the first place. Finally, Scenario 4 would see an increment in the market, perhaps there would be an even greater need for a secondary trading network but other solutions would be required because of the antagonist sentiment of the regulator. Concluding this part, is clear how Scenario 2 and 3 are equally detrimental for the whole project, while the fourth one would simply enhance the actual status quo. In the next chapter, this work will devise a concept and a strategy capable to increase as much as possible the chances for Scenario 1 to prevail over the other three.

3 Proof of concept: Methodology and Results

In this chapter, the author will finally merge what has been learned from the literature reviews and from the scenario planning. The concept the author is going to expose, completed with some guidelines, and are meant to maximize the probability of having in the future a “Scenario 4” situation, of course respecting all the boundaries in term of technical capabilities of the technology involved and the dynamics studied for crowdfunding platform and campaigns.

Stephanie Houde and Charles Hill (Hill & Houde, 1997) wrote prototyping is a widely recognized way to explore and design interactive computer artefacts. However, complexity of different artefacts may create issues regarding what kind of proof of concept framework, for instance story telling or actual physical model of the final product. The paper introduced a model composed by three main dimensions for prototyping, functions that an artefact serves in a user’s life, the concrete sensory experience of using an artefact and the techniques and components through which an artefact performs its function, for the authors all dimensions are equally important and in trade off one with another when it comes to choose which solution to implement when defining the proof of concept. When the it is wanted to use a framework able to address all the dimensions the authors refer to that as “integration”.

In order to pick the best framework, firstly it has to been understood what are the weights this work will assign to the three different dimensions. The paper gives to the reader, in its conclusions, a checklist of practical suggestion needed to assess the best framework:

- Define “prototype” broadly. Efficient prototypes produce answers to their designers’ most important questions in the least amount of time. Sometimes very simple representations make highly effective prototypes.
- Build multiple prototypes. Since interactive artefacts can be very complex, it may be impossible to create an integrated prototype in the formative stages of a project.

- Know your audience. The necessary resolution and fidelity of a prototype may depend most on the nature of its audience.
- Know your prototype; prepare your audience. Be clear about what design questions are being explored with a given prototype—and what are not.

Starting from the question this section aims to answer: “It is possible to implement a secondary market for crowdinvesting using distributed ledger solutions”. In order to answer this question the prototype should show the functions it is going to cover and the technological feasibility, also because the “user experience” is not going to be revolutionised by the system. This thesis was meant for management engineers likewise the author therefore there will be technicalities, understandable thanks to the literature review, but held on a medium level, no code for instance. The proof of concept framework chosen for this work will be a Process Flow-Prototype storyboard that will represent several situations which end users, investors, platforms and entrepreneur, are more likely to encounter, showing the technological dynamics of the proposed system.

3.1 Creation of a security based crowdfunding campaign

In Fig.[] it is showed how a campaign starts in the consortium. When a start-up or a SME wants to ask for capitals through a security based campaign, it has to reach a portal providing it with the business plan and all the due documentation. If the proposition is accepted, the issuer will create a copy of cryptographic keys that will be its way to interact on the network. The platform that accepted the company for a crowdfund will create a smart contract with all the details of the incoming campaign such as the public address of the issuer, the minimum amount asked to trigger the money transfer, the dead line, the escrows’ address where investors can deposit their commitments. The escrow is then sent to the “validation pool” where it can be picked by any node empowered by the prerogatives of “validator”, for example a platform member of the consortium or an exchange. Any validator node’s identity is known to its peers, therefore it is possible to implement a consensus system based upon the Practical Byzantine Fault Tolerance, similar to Ripple’s one. Every validator has its own unique list of other nodes with the same authority built in order to lower as much as possible the probability of collusion hence the probability of an attack direct to the consensus as seen in Fig. [47].

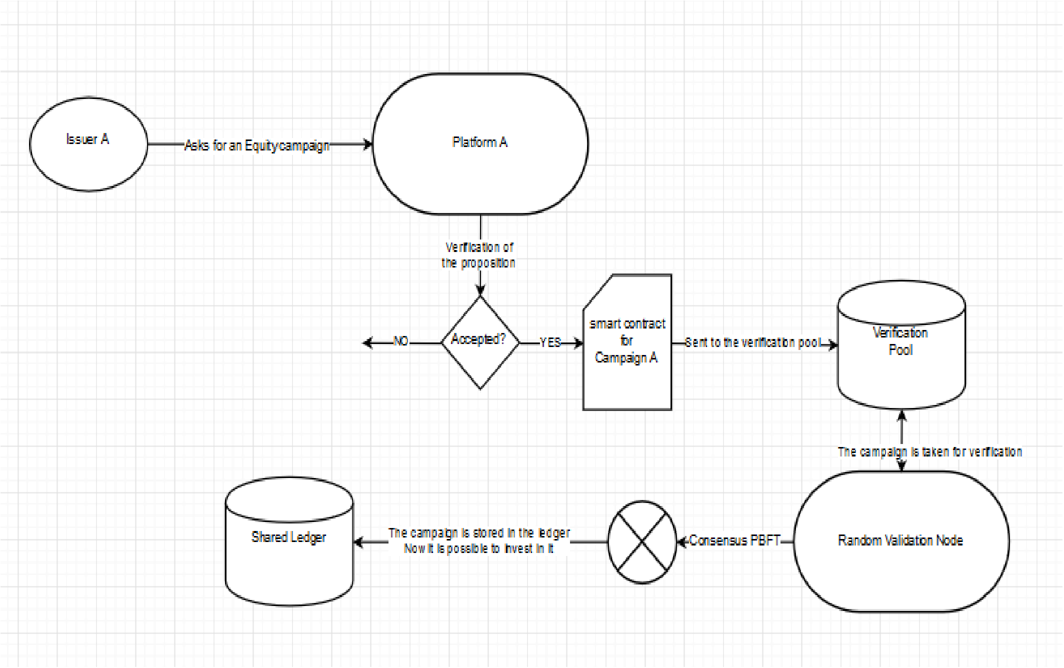

Issuer A
Asks for an Equitycampaign
Platform A
Verification of the proposition
NO
Accepted?
YES
smart contract for Campaign A
Sent to the verification pool
Verification Pool
The campaign is taken for verification
Random Validation Node
Consensus PBFT
The campaign is stored in the ledger Now it is possible to invest in it
Shared Ledger

Figure 47 Flowchart for a newly accepted campaign

Now the campaign is advertised on the chosen crowdfunding platform and the escrow where to put the money has been provided. The only problem is: What kind of money/currency does this system accept? For this project I consider a native currency called for the occasion CrowdCoin.

The system has now a currency that can be committed to a campaign. The investor Bob wants to participate investing some of its saving in a campaign. To do so he as to acquire the value intended to be invested in CrowdCoins. For this reason he can contact any person willing to make an exchange, another investor or a platform Fig.[]. Alice is willing to make the exchange so she send the transaction of X Coins from her address to Bob's one. This time the network receives a transaction, instead of a contract as before, therefore the process is slightly different because it involves a consensus based upon Proof of Work instead of PBFT. In this way it is possible to implement a non-deterministic way to mint the native currency, as in Bitcoin. Furthermore, miners are the same validators as for before therefore they are crowdfunding platforms or other companies that are not depending on mining as primary source of revenues, this should prevent the escalation of resources for mining Fig [48] as it happens in Bitcoin. The cost of Mining is the price for the hardware and instalment plus the maintenance minus the value of the coins minted, while the cost of concentration takes into account the missed profits from not having mined, the costs related to the risk of a concertation of mining and its reflection in the value of the currency itself.

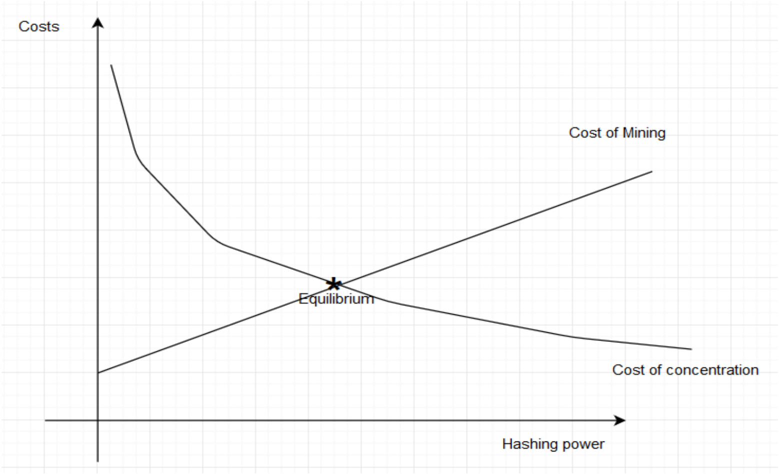


Figure 48 Representation of the trade-off between spending resources for mining and letting the mining to third parties

We have seen in the literature how important the process of verification by a financial institution is. This process, which has been labelled as know your customer, is also a source of expenditure because every entity must repeat the same process every time the client want to open an account with a new bank or another financial intermediary. We have seen how crowdinvesting is not exempted from such burden; hence, clients must fill every time the same set of forms and provide the same requested information. This may result into an unpleasant redundancy both for clients and for platforms. A sub-chapter of the literature review explained how shared ledgers might be again a viable and efficient solution also for this matter by using cryptography and private keys is possible to spread information through the entire network while preserving the privacy of the clientele. In the case depicted both Bob and Platform A, which profiled Bob, hold the key capable to decrypt Bob’s file. Platform B just should ask Bob for the key in order to obtain the same information instantly and, only if platform B is not satisfied with the work already done by A, asking for a new KYC process or just asking for additional information.

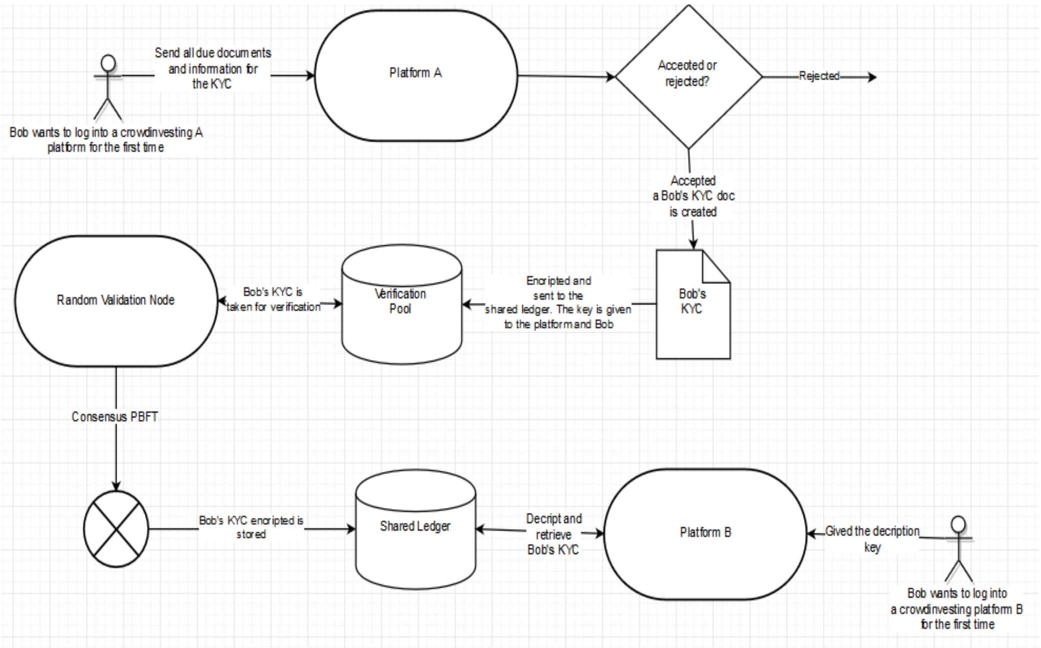

Send all due documents and information for the KYC
Bob wants to log into a crowdinvesting A platform for the first time
Platform A
Acceoted or rejected?
Rejected
Accepted a Bob's KYC doc is created
Bob's KYC
Encripted and sent to the shared ledger. The key is given to the platform and Bob
Verification Pool
Bob's KYC is taken for verification
Random Validation Node
Consensus PBFT
Bob's KYC encripted is stored
Shared Ledger
Decript and retrieve Bob's KYC
Platform B
Gived the decription key
Bob wants to log into a crowdinvesting platform B for the first time

Figure 49 Flowchart for the shared KYC process

The way transactions of coins and securities’ ownership through tokens is depicted as Fig.[50]. Bob wants to back up a campaign of its choosing but to do so he needs coins which can be obtained buying them from platforms or from other users, as in the case depicted.

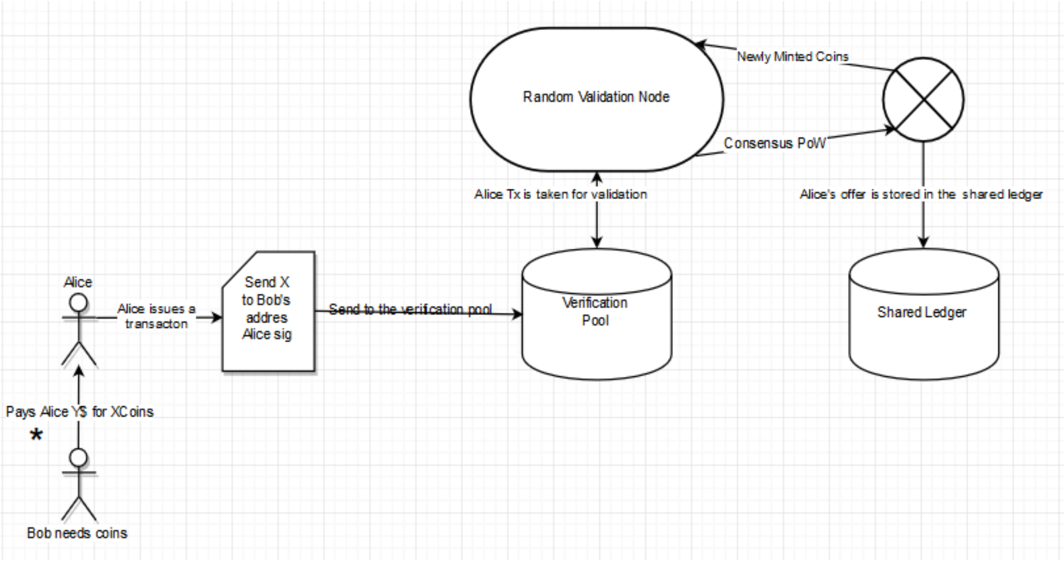

Random Validation Node
Newly Minted Coins
Consensus PoW
Alice Tx is taken for validation
Alice's offer is stored in the shared ledger
Alice
Alice issues a transacton
Send X to Bob's addres Alice sig
Send to the verification pool
Verification Pool
Shared Ledger
Pays Alice Y$ for XCoins
*
Bob needs coins

Figure 50 Flowchart for a coin transaction

Now Bob has the coins to invest into the target campaign, he has to find some opportunities to invest in. For this purpose, the concept implements a distributed ledger that is permissioned, since not all nodes can be validators at will, but public meaning that anyone can see and download the ledger at any time. Finally, Bob found an interesting opportunity in an ongoing campaign ad decides to finance it with part of its coins. The procedure for backing a campaign is similar to a normal transaction, actually is by any mean no different from a transaction. Therefore the process is just as showed in the previous Fig.[51]. Now the commitment is stored into the ledger and Bob just has to wait until the campaign is over. In the meantime, Alice decided to disinvest from a position of here. Alice does not know anybody interested in take over her position therefore; she is experiencing the typical illiquidity of crowdinvesting. She decides to issue a smart contract into the shared ledger to advertising her willingness of liquidate her investment.

This time the situation is similar to the first one since it deals with smart contracts therefore the process will not be similar to the transitive ones. Alice broadcast to the verification pool her offer signed with her public key and hashing it as Id of the contract, then the process proceed as in Fig.[]

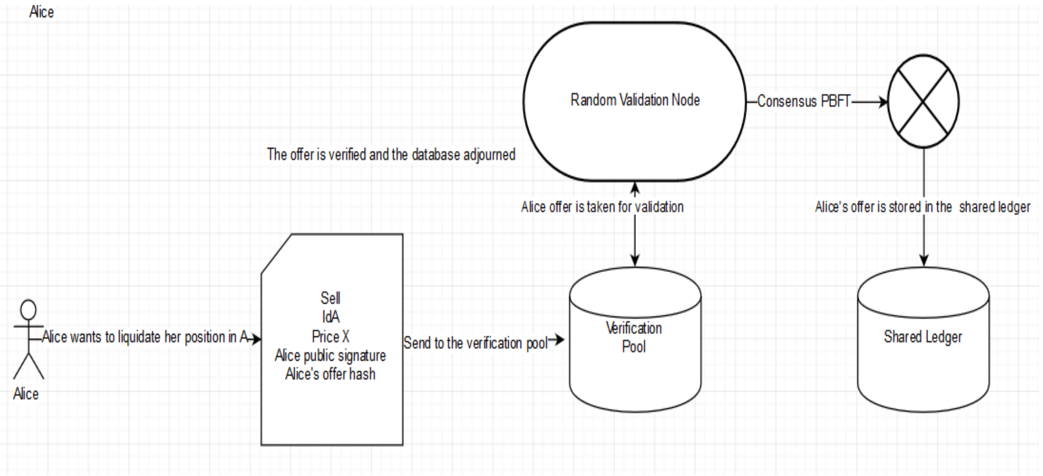

Alice
Random Validation Node
Consensus PBFT
The offer is verified and the database adjourned
Alice offer is taken for validation
Alice's offer is stored in the shared ledger
Sell
IdA
Price X
Alice public signature
Alice's offer hash
Alice wants to liquidate her position in A
Send to the verification pool
Verification
Pool
Shared Ledger
Alice

Figure 51 Flowchart of an on ledger offer

Now her offer is of public dominion and every possible investor interested in it can issue another contract. It happened to be Bob as in Fig.[52]. This time the system is again dealing with something more complex than a mere transaction, but in the end is nothing more than a double transaction since the payment of the asked price triggers the change of ownership of the securities. Therefore, the protocol implemented for this kind of operation is the PoW.

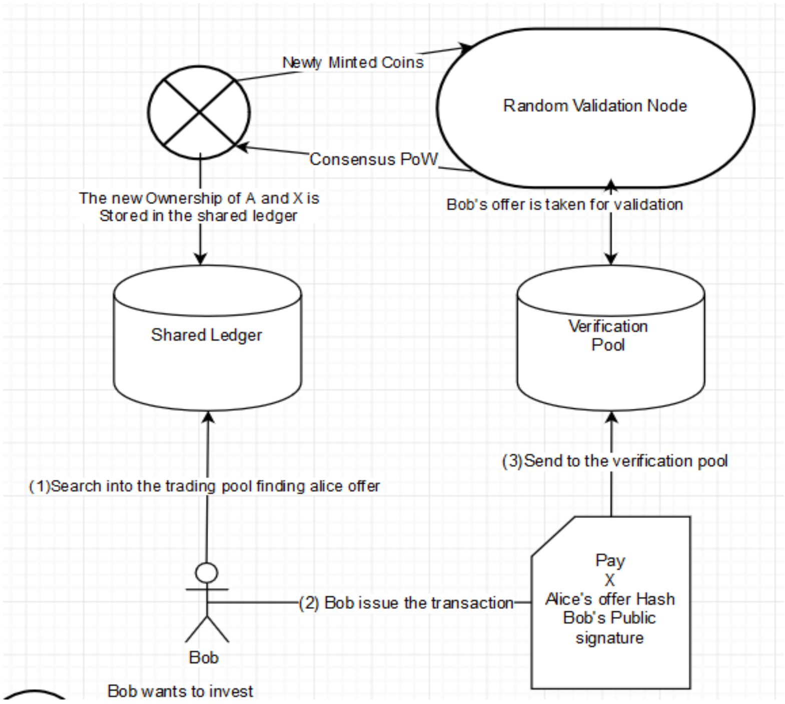

Newly Minted Coins
Random Validation Node
Consensus PoW
The new Ownership of A and X is Stored in the shared ledger
Bob's offer is taken for validation
Shared Ledger
Verification Pool
(3)Send to the verification pool
(1)Search into the trading pool finding alice offer
Pay
X
Alice's offer Hash
Bob's Public signature
(2) Bob issue the transaction
Bob
Bob wants to invest

Figure 52 Flowchart of an on chain purchase of securities

At the end of a campaign, at its due date, the platform which the company chose to issue its fundraising retrieves the escrow from the shared ledger and it rebroadcast again to the networks' verification pool. All validators can check that all the requirements expressed on the contract have been fulfilled and then they can finally reach a PBFT consensus to distribute the capital to the firm and the tokens of the issued securities at the investors' addresses as showed in Fig.[53] the firm will obtain the funds by selling the Coins on the market. It would be possible to set a goal in terms of any particular fiat currency and pegging the value of the final funds raised to the spot rate expressed that day on websites like Coindesk or Bitstamp or Coinbase. During the period of transition the presence of custodians will be necessary because of the, presumably, very low value and high volatility of the coin, as expected from a cryptocurrency (Dourado & Brito, 2014).

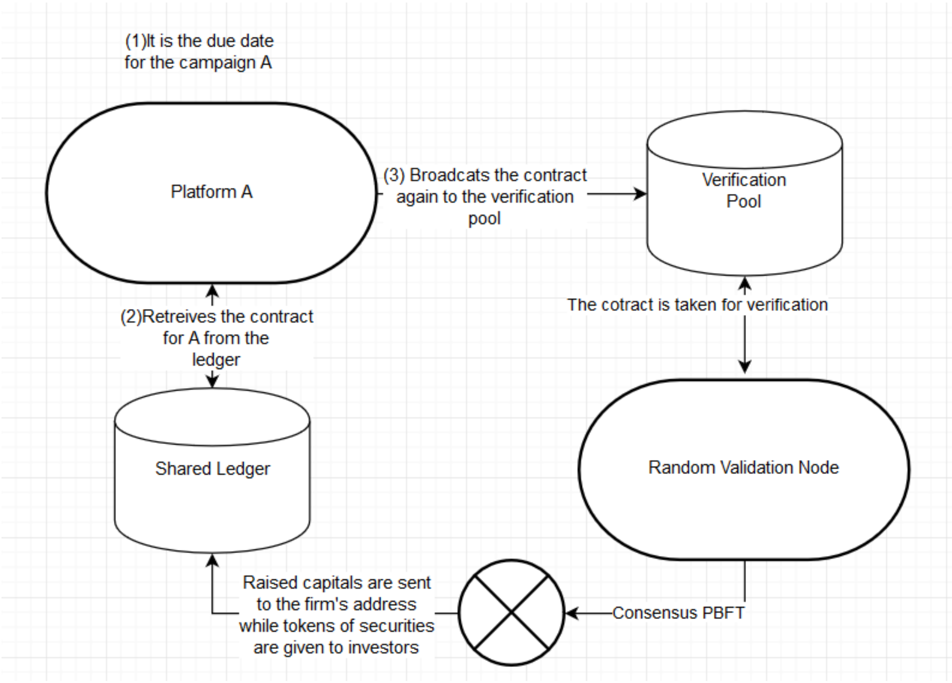


Figure 53 Flowchart of a successful campaign at the due date

In order to enhance the protection of investors interests, the author proposes some expedients, realizable cheaply only through a distributed ledger, capable to address some of the issues highlighted during the literature review. First of all we described in the literature review several exempla of instruments that can be used to control the direction of the funded company and align it with the interests of the crowd. One of the most promising is staged financing, the process to link the transfer of capitals in trances linked to future conditions pre negotiated during the campaign. This system would require to pay a financial institution to act as custodian for many months after the end of the campaign with adjunctive costs for the issuer. With a system based upon DLT that expense would be avoided by simply adding few lines of codes to the contract. Another instrument can be seen into golden shares, particular stocks that grant the holder privileged voting rights. The issuer may propose, for a certain period of time to grant the crowd with the majority of the voting, keeping the majority of the property, for particular matters such as acquisitions, sells of activities or ask for more capitals through VCs or crowdfunding. Finally the issuer can keep its cash as cryptocurrency and ask to the crowd anytime it has to make a payment greater than a certain previously accorded threshold. In Fig. [] this work demonstrates how such system can be implemented.

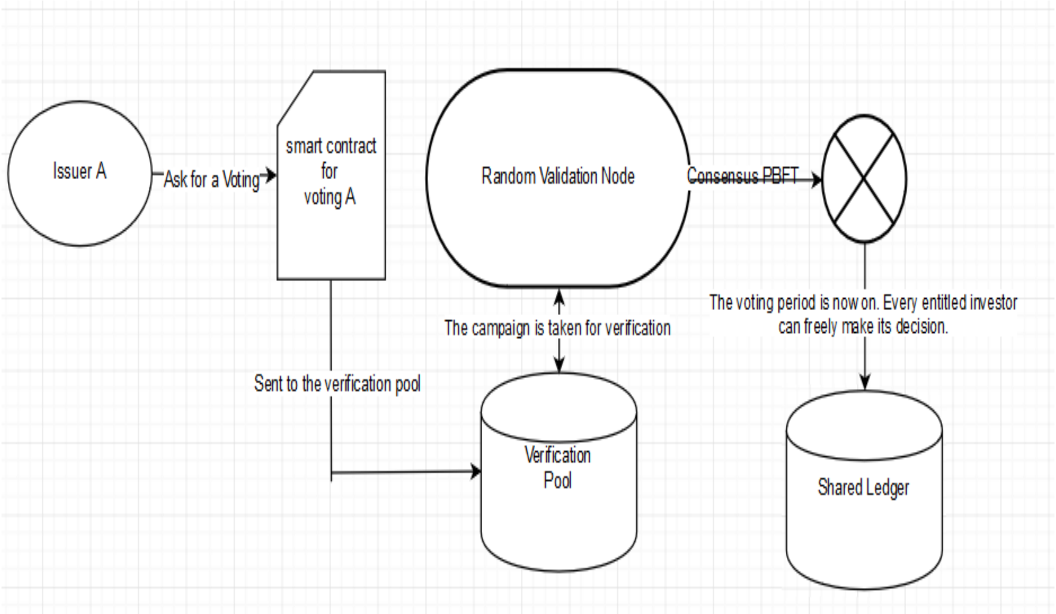

Issuer A
Ask for a Voting
smart contract for voting A
Random Validation Node
Consensus PBFT
The voting period is now on. Every entitled investor can freely make its decision.
The campaign is taken for verification
Sent to the verification pool
Verification Pool
Shared Ledger

Figure 54 An issuer ask its investors' network for a voting

The Issuer can propose everything previously agreed, it can ask for releasing the next share of a staged financing, the crowd has the right to assess its results so far and decide whether or not to grant the capital, in case investors are not satisfied with the issuer's performance the smart contract would issue a transaction repaying the crowd with the fund's remains. Another exemplum would be to propose to go through another round of crowdfunding issuing new shares or new debt and so on. Thanks to the distribution of the network it would be extremely easily for every investor to vote and, thanks to the excellent notary system that blockchain is, it would be confident its vote has been registered and posed outside any possible fraud attempt.

Taken example from Factom it would be possible to implement a notary system for this distributed ledger by engraving it into Bitcoin, which is by dimension way more tamper resistant than this network. The system of this work has an inner decentralised clock that is its blockchain, based on proof of work. Therefore it would be possible to set a frequency like every X blocks all nodes presents an hashed time stamped, with the hash of the nX block, Fig[54] and try to solve a PoW in order to have their version globally accepted Fig. [55]. After that the winning version of the ledger is sent to the Bitcoin network as a dummy transaction in order to be picked by miners and added to the Blockchain as a safe and globally accepted milestone. In this way, all nodes are forced to maintain a high level of similitude in order to be compliant with what stored on Bitcoin

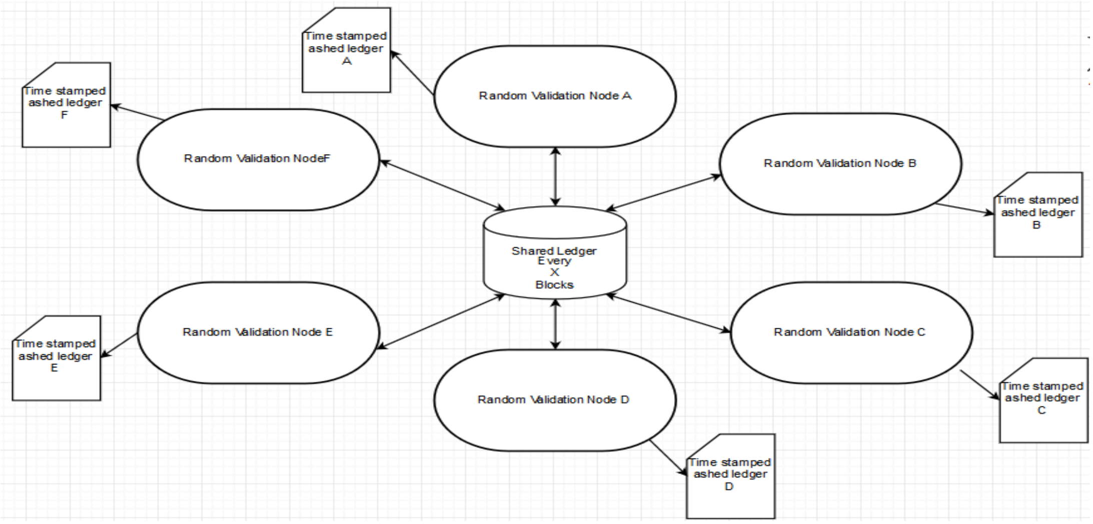

Time stamped ashed ledger A
Time stamped ashed ledger F
Random Validation Node A
Random Validation NodeF
Random Validation Node B
Time stamped ashed ledger B
Shared Ledger Every X Blocks
Random Validation Node E
Time stamped ashed ledger E
Random Validation Node C
Random Validation Node D
Time stamped ashed ledger C
Time stamped ashed ledger D

Figure 55 Every X blocks all validators present to the network their timestamped hashed ledger

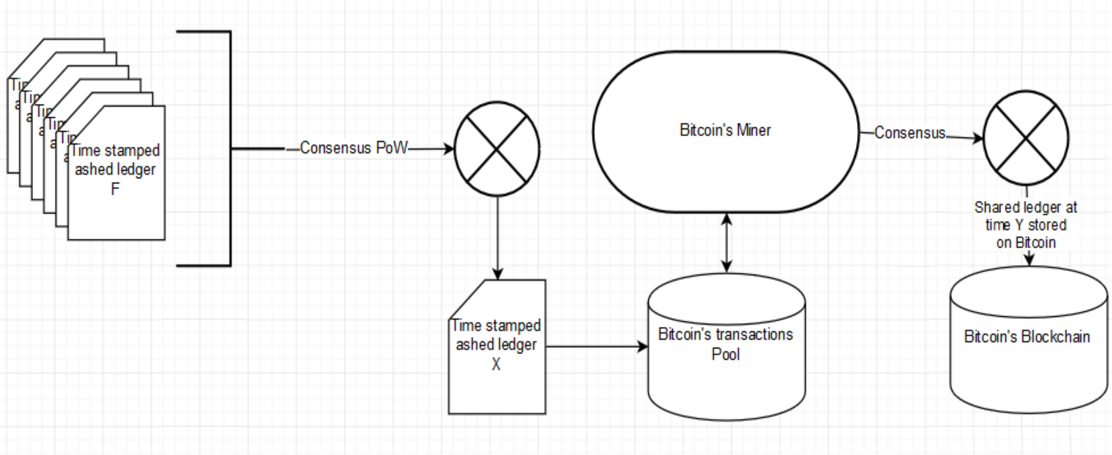

Time stamped ashed ledger F
Consensus PoW
Bitcoin's Miner
Consensus
Shared ledger at time Y stored on Bitcoin
Time stamped ashed ledger X
Bitcoin's transactions Pool
Bitcoin's Blockchain

Figure 56 The winning ledger is sorted out through PoW and then sent to the Bitcoin network

Finally the system must be compliant with the future position of regulatory authorities therefore it is important that all validator nodes are firstly known to the public entity and secondly fully able to provide information in case of ongoing investigations for issues taken into consideration in the crowdfunding part of the literature review, money loundering, frauds and so forth. On the same time, the regulator must acknowledge the properties rights stored on the ledger and proceed to enforcement the rights of all parties in case of litigation as for every traditional case. The disclosure of validator nodes is not negotiable, for all the other nodes it could be preserved the pseudo anonymity or they may be forced to disclose their information for legal and tax purposes. The disclosure of normal nodes might be a source of friction for a major use of coins not just for crowd related operations but also for daily routine. . The best way to proceed with the actual implementation of this project would start with the realization of the network within a sandbox, an isolated virtual environment where it is possible to directly intervene upon different variables assessing how the system react to different sources of stress. A sandbox does not put information or sensible data at stake of platform's costumers at risk since it is not yet integrated with the external environment. "During this phase the seed of what could become the consortium has not to be already numerous, as a matter of fact a large number of actors could pose an unnecessary complexity for the realisation of the project".

3.2 Validation

In order to validate this concept the author asked the opinion of experts, both from the distributed ledger technology side as well as from the crowdinvesting one, and from the market. Marco Monaco is Blockchain Practice Leader at PricewaterhouseCoopers and he was so kind to review this work of thesis and its Proof of Concept. Marco's first concern about the PoC was the use of a double consensus protocol within the same ledger: "The technical part was done thoroughly, but why do you decided to implement two different protocols, PBFT for contracts and PoW for transactions? You could have just used a single PBFT capable to read transactions upon the Bitcoin's Blockchain". To the question the author answered, "The use of a double system was conceived in order to have both the vantages of PBFT scalability and PoW censorship and tamper resistance, also to rely upon a clock for timestamping”. To this, Marco replied: “Then why not use Bitccoin for value transfer and time stamping and Ethereum for smart contracts?” My reply was that interviewed platforms strongly agreed to desire to have a permissioned network, also for compliance with the regulator. Another doubt raised was concerning enforcement of investors rights: “ICOs are difficult to manage for investors because there is no real way for them to enforce their rights after a campaign is done. I expected to see some consideration about this matter here”. To his remark, I replied the system doesn’t deals with ICOs but with actual crowdfunding campaigns, with platforms ad laws. The system was devised to combine the tokenisation and tradability if ICOs with institutional solidity and rule of law of traditional crowdinvesting. Marco agreed with my explanation. A last personal remark of Marco is this work of thesis significantly solidified his impression that crowdfunding is one Killer App for distributed ledger platforms. One of his main concern was about the management of identities and private keys. The solution proposed is that private key generation is left to the client, investors and campaigners, but in order to be able to participate to campaigns or to invest, during the KYC phase the public address must be provided to the querying platform. Platforms will be then able to respond to public authorities in case of investigations but the private key will remain a secret known only to the owner of the associated account.

To the interviewed platforms’ spokespeople, it was asked to express their opinion about the real capability of a secondary market to address issues highlighted during the literature review, in order to solidify the results showed searching for benefits of secondary markets. The possibility to trade efficiently has been sees as a solution for the illiquidity of such assets, also signals coming from prices have been seen as a way to partially overcome asymmetries. The possibility to trade on a secondary market would allow for an enhanced level of diversification in investors’ portfolios, attracted also by the single platform for multiple asset classes, hence decreasing risk connected to a certain expected return. Another aspect the author wanted to understand by asking feedback from crowdfunding platforms was about the eventuality to join a consortium, to allow their clients to easily trade their assets. Respondents expressed their willingness and interest towards such solution, even having to cope with competitors, and their willingness, in case of a favourable scenario, especially concerning regulation and growth of the primary market, to invest funds to create it. Massimo Masserdotti of Tip Ventures was more cautious stating that the Italian current market size and regulation would make him wary to commit to such endeavour, while a context closer to the American one or at least to the English one would make him more prone to enter in the consortium. Overall, the reception ranged from the cautiously inclined to the extremely interested. The author, however, noted a significate lack of comprehension of blockchain and the paradigms underneath it.

4 Conclusions and Further research

Crowdinvesting is the for profit and by far the most rich definition of the crowdfunding phenomenon. Crowdinvesting itself can be divided into three other main categories, equity crowdfunding, peer to peer lending and invoice trading. This alternative way for start-ups and SMEs to finance themselves bloomed after great financial crisis like the subprime and the sovereign debt ones because of the subsequent lack of credit for riskier enterprises. Growth's momentum for crowdinvesting is still strong but there are important reasons to believe major frictions are acting against it. From the literature revised this work concluded that illiquidity, uncertainty in future value of assets, and difficulties to establish fair prices, lack of information and extreme skewness in how it is distributed among different actors, with the crowd, usually left mostly unaware, are major drawbacks for the growth of crowdinvesting industry.

This work aimed to find a viable source to address and eliminate, or at least mitigate, said sources of friction. The revision of the academic review and feedback provided directly by experts and entrepreneurs from the industry suggested liquid and as much as possible efficient secondary markets where trading crowd based assets may provide an answer to all the issues discovered. This work rapidly realised how traditional infrastructure, used in financial markets, would have required investments, technical and managerial know how unthinkable for an industry this small. The revision brought to the attention of the author an extremely new way to perform crowdinvesting like campaign, the initial coin offers, performed using a set of technologies falling beneath the umbrella definition of "distributed ledger technology". This work explored thoroughly the topic of distributed ledger technologies. The author tried to provide himself and the reader with a narration starting from the very scientific and technological fundamentals behind distributed ledger solutions, in order to be able to understand and revise the actual most prominent services available, the economical and jurisdictional aspects and the actual the most probable future applications. This research suggest the primary role of the right matching of consensus protocols and system's features desired. The first guideline would be that it is of paramount importance to be completely clear about parameters such as number of participants to the network, availability of the ledger, access to maintenance and to modification of the protocol and the ledger, desired resistance towards censorship and immutability of the ledger and so forth.

Since illiquidity, information asymmetries and transaction costs are all market's failure, this work studied academic literature about how blockchains are able to tackle these issues. Result showed Distributed Ledger solutions are able to address in a very efficient and effective way problems related with "hidden action" and "moral hazard" issues because of the capability for everyone entitled, for example a regulator, to monetarise in real time cash flows and change of ownership, creating useful signals for the whole market. Transaction costs are lowered by the, future, possibility to overcome the need of notaries, custodians and by having offer and demand meet on a common ground. A useful guideline would be to implement a consortium solution in order to maximise the network externalities and the economies of scale.

From the study of different regulators‘ current tendencies towards the possibility to implement solutions based upon distributed ledgers this work defined that public but permissioned distributed ledger network are the most promising to meet their taste, hence their approval. Permissioned networks allow the definition of a structure well posed legal and governance structure. Another concerning aspect when this work refers to regulator is the management of user information and privacy. For these aspects, the approach cannot be of full anonymity such as monero or Zcash nor pseudonymity such as Bitcoin, a solution that would be of authorities' preference would be a personal ID associated with a public address that is known to the platform that performed the KYC and to the regulator in case of investigation.

This research eventually searched within the literature gathered for the main issues and threats recalled by all the different contributors compiling a P.E.S.T analysis with the purpose to know what would have been useful to ask to experts from both the crowdinvesting field as well as from the Distributed Ledger one. These efforts were necessary in order to understand which factors, trend and uncertainties were felt as the most concerning for the eventual combination of crowdinvesting and distributed ledger technology into a viable technological and operational solution. From what the author understood by studying the results of the P.E.S.T analysis and the feedback from the respondents it appeared clear regulators are the greatest source of threat because of their significant impact factor and their unpredictability. The piece of advice the author is confident to give would be to work as close as possible with the regulator, placing great effort to maintain an open communication channel in order to be able to receive loud and clear any new directive while keeping it adjourned.

Lastly, this work provided the reader with a proof of concept, a preliminary blueprint, of a probable distributed secondary market for crowd based assets. This part is the results of all the previous research from secondary and primary sources and of the guidelines and insight extrapolated from them. In this prototype the author simulated all the most important situations occurring to all possible involved parties, platforms, capital seekers and investors, within a network conceived as an original and innovative, since nothing like that exist yet, distributed ledger consortium managed by accredited nodes, platforms and possibly known outsourcers. The originality of this work resides on the fact for the first time a research proposed not only the necessity of a secondary market but also a technical viable solution to provided it. Another point of originality is the proposed secondary market run above a distributed ledger consortium, never proposed before, where it is possible to launch new campaigns, invest in them, be certain the committed capitals will go to the campaigners or returned to the crowd without having to rely upon trusted third parties and so on. The prototype has been proposed to a technical validation by experts who approved overall the applicability of such solution, the concept received interest also by the experts from the crowdfunding arena who expressed, if certain conditions, especially concerning to regulation, where met, they willingness to associate and invest in a consortium such as the one devised. Another point of innovation was to combine all different declinations of crowdinvesting, meaning equity alongside p2p lending alongside invoice trading, and extend the consortium towards a European scale.

Future research may address and tackle more deeply the trends and uncertainties discovered, by increasing the pool and variety of experts reached, this can potentially lead to the creation of new scenarios which this work has not taken into consideration, hence in significant modification of the prototype and standards. The author advice also to further study the governance schemes a consortium as the one proposed should adopt, in order to fully overcome issues related to conflict of interests, free riding and interaction with the regulator. Future research should extent this work towards a European, at least, horizon in order to catch all the possible opportunities of network and diversification of investment opportunities.

Images Index

Index of Tables

Bibliography and Online sources

Agrawal, & al. (2013). SOME SIMPLE ECONOMICS OF CROWDFUNDING. *NBER WORKING PAPER SERIES*.

Agrawal, & al. (2015). Crowdfunding: Geography, social networks, and the timing of investment decisions. *Journal of Economics & Management Strategy*, 253-274.

Aguilar, L. A. (2017, 04 1). *The Need for Greater Secondary Market Liquidity for Small Businesses*. Tratto da sec.gov: https://www.sec.gov/news/statement/need-for-greater-secondary-market-liquidity-for-small-businesses.html

Akentiev, A. (2017, 03 12). *Hyperledger vs Corda Pt.1*. Tratto da medium.com: https://medium.com/chain-cloud-company-blog/hyperledger-vs-corda-pt-1-3723c4fa5028#.wcij5zxtx

Alchemi. (2016, 12 28). *Solution to Sybil attacks and 51% attacks in Decentralized Networks*. Tratto da LetsTalkBitcoin: https://letstalkbitcoin.com/blog/post/solution-to-sybil-attacks-and-51-attacks-in-decentralized-networks

Alcoins.com. (2017, 03 15). *Scamcoins*. Tratto da altcoins.com: http://altcoins.com/scamcoins

Alegre, I., & Moleskis, M. (2016). *Crowdfunding a review and research agenda.*

Ametrano, F. (2016, 12 31). *Hayek money: the cryptocurrency price stability solution.* Tratto da SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270

Amy, M., & al. (2016). Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. *Cryptology ePrint Archive: Report 2016/992*.

Anand, A., & al. (03/2016). Colored Coins: Bitcoin, Blockchain, and Land Administration. *Annual world bank converence on land and poverty.* Washington DC.

Anderson, L., & al. (6/2016). *New kids on the block: an analysis of modern blockchains.* Cornell University Library.

Antonopoulos, A. (11/2015). *Mastering Bitcoin.* O'Reilly Media.

Armknecht, F., & al. (8/2015). Ripple: Overview and Outlook. *Lecture Notes in Computer Science*, pp 163-180.

Ateniese, G., & al. (2016). Redactable Blockchain or Rewriting History in Bitcoin and Friends. *IARC Cryptology ePrint Archive*, 756.

Back, A., & al. (2014). *Enabling Blockchain Innovations with Pegged Sidechains.*

Badreddin, O. (2013). Empirical evaluation of research prototypes at variable stages of maturity. *2013 2nd International Workshop on User Evaluations for Software Engineering Researchers (USER).*

Badreddin, O., & Lethbridge, T. (2012). Combining experiments and grounded theory to evaluate a research prototype: Lessons from the umple model-oriented programming technology. *2012 First International Workshop on User Evaluation for Software Engineering Researchers (USER).*

Bartoletti, M., & Pompianu, L. (03/2017). *An analysis of Bitcoin OP RETURN metadata.* arXiv.

Baucus, M., & Mitteness, C. (2016). Crowdfrauding: Avoiding Ponzi entrepreneurs when investing in new ventures. *Business Horizons* .

Belleflamme, & al. (2013). *Individual Crowdfunding Practices.*

Belleflamme, P., & al. (2010). *Crowdfunding: An Industrial Organization Perspective.*

Belleflamme, P., & al. (2013). Crowdfunding: Tapping the right crowd. *Journal of Business Venturing*.

Belleflamme, P., & Lambert, T. (2013). *Crowdfunding: Some Empirical Findings and Microeconomic Underpinnings.*

Benjamin Johnson, &. a. (10/2014). Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools. *Volume 8438 of the book series Lecture Notes in Computer Science (LNCS).*

Benjamin, L., & Schwienbacher, A. (2012). CROWDFUNDING OF SMALL ENTREPRENEURIAL VENTURES. In *Handbook of Entrepreneurial Finance.* Oxford University Press.

Bertani, T. (2017, 02 19). *Understanding oracles.* Tratto da Oraclize.it: https://blog.oraclize.it/understanding-oracles-99055c9c9f7b#.w64vqar58

Biella, M., & Zinetti, V. (2/2016). *Blockchain Technology and Applications from a financial perspective.* Unicredit.

Bitcoinblockhalf.com. (2016, 12 29). *Bitcoin Block Reward Halving Countdown*. Tratto da bitcoinblockhalf: http://www.bitcoinblockhalf.com/

Bitfury. (2016). *Digital Assets on Public Blockchains.* BitFury Group.

Bjerg, O. (12/2015). How is Bitcoin Money? *Theory, Culture & Society, Vol 33, Issue 1*, 53-72.

Boroujerdi, R. D., & Wolf, C. (12/2015). *What if I Told You ... the Blockchain Could Disrupt ... Everything.* Goldman Sachs Global Investment Research.

Bouncken, R. B., & Kraus, S. (2015). Crowdfunding: The Current State Of Research. *International Journal of Economics and Business Research*.

Bradbury, D. (2016, 12 20). *Chris Larsen: Ripple is HTTP for money*. Tratto da CoinDesk: http://www.coindesk.com/chris-larsen-ripple-is-http-for-money/

Braendgaard, P. (2017, 02 19). *Simple Convention for Human Readable Terms for Smart Contracts.* Tratto da StakeVentures: https://blog.stakeventures.com/articles/smart-contract-terms

Brown, R. G. (2016, 12 18). *Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services*. Tratto da r3cev.com: http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

Brown, R. G. (2017, 04 15). *A simple model to make sense of the proliferation of distributed ledger, smart contract and cryptocurrency projects*. Tratto da gendal.me: https://gendal.me/2014/12/19/a-simple-model-to-make-sense-of-the-proliferation-of-distributed-ledger-smart-contract-and-cryptocurrency-projects/

Buterin, V. (2012). *White Paper: A next generation smart contract & decentralized application platform.* Ethereum Foundation.

Buterin, V. (2016, 12 20). *Ripple is officially open source*. Tratto da Bitcoin Magazine: https://bitcoinmagazine.com/articles/ripple-is-officially-open-source-1380246874

Buterin, V. (2016, 12 03). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*. Tratto da Ethereum blog: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Buterin, V. (2017, 02 25). *a next generation smart contract & decentralized application platform.* Tratto da fintech.academy: http://www.fintech.academy/wp-content/uploads/2016/06/EthereumWhitePaper.pdf

Buterin, V. (2017, 02 25). *SchellingCoin: A Minimal-Trust Universal Data Feed.* Tratto da ethereum.org: https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/

Buysere, K. d., & Hooghiemstra, S. N. (2016). The Perfect Regulation of Crowdfunding: What Should the European Regulator Do? In D. Brüntje, & O. Gajda, *Crowdfunding in Europe* (p. 135-165). Springer .

Cachin, C., & al. (2001). Secure and efficient asynchronous. *Advances in Cryptology: CRYPTO*, 524-541.

Cai, J., & al. (2015). Information Asymmetry and Corporate Governance. *Quarterly Journal of Finance*.

Cermeno, J. (12/2016). *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application.* BBVA research.

Chan, R. (2016, 11 01). *Consensus mechanism used in Blockchains*. Tratto da Linkedin: https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-chan

Charles, B., & Lunn, W. (2016). *Blockchain.* Credit suisse.

Chepurnoy, A. (1/2016). *Interactive Proof-of-stake.* Cornell Unversity Library.

Chuen, D. L. (2015). HANDBOOK OF DIGITAL CURRENCY: Bitcoin, Innovation, Financial Instruments, and Big Data. Elsevier.

Clack, C. D., & Bakshi, V. A. (08/2016). Smart Contract Templates: foundations, design landscape and research directions. *eprint arXiv*.

Clack, C. D., & Bakshi, V. A. (12/2016). Smart Contract Templates: essential requirements and design options. *eprint arXiv*.

Commission, E. (11/2016). *SMALL AND MEDIUM SIZED ENTERPRISES' ACCESS TO FINANCE.* EUROPEAN SEMESTER THEMATIC FACTSHEET.

Condos, J., Sorrell, W., & Donegan, S. (1/2016). *Blockchain Technology: Opportunities and risks.* Stete of Vermont.

Consob. (08/2016). *L'equity-crowdfunding Analisi sintetica della normativa e aspetti operativi.* CONSOB.

Consob. (2013). *Regolamento sulla raccolta di capitali di rischio tramite portali on-line.* Consob.

contributors, W. (2016, 12 29). *Merkle tree*. Tratto da Wikipedia, The Free Encyclopedia: https://en.wikipedia.org/w/index.php?title=Merkle_tree&oldid=751143973

contributors, W. (2016, 12 18). *R3 (company)* . Tratto da Wikipedia, The Free Encyclopedia. : https://en.wikipedia.org/w/index.php?title=R3_(company)&oldid=754973942

contributors, W. (2017, 03 18). *Escrow* . Tratto da Wikipedia, The Free Encyclopedia: https://en.wikipedia.org/w/index.php?title=Escrow&oldid=766781939

Correia, M., & al. (2011). Byzantine consensus in asynchronous message-passing systems: a survey. *Int. J. Critical Computer-Based Systems, Vol. 2, No. 2*, 141-161.

Croman, K., & al. (2/2016). *On Scaling Decentralized Blockchains.* ETH.

Croman, K., & al. (2016, 12 30). *On Scaling Decentralized Blockchains.* Tratto da Financial Cryptography and Data Security 2016: http://fc16.ifca.ai/

Crosby, M., & al. (2015). *BlockChain Technology.* Sutardja Center for Entrepreneurship & Technology Technical Report.

Crowdexpert.com. (2017, 03 19). *Crowdfunding Industry Statistics 2015 2016*. Tratto da Crowdexpert.com: http://crowdexpert.com/crowdfunding-industry-statistics/

CrowdFundBeat. (2017, 03 20). *Report: Global Crowdfunding Market 2016-2020*. Tratto da CrowdFundBeat : http://crowdfundbeat.com/2016/02/03/report-global-crowdfunding-market-2016-2020/

CrowdfundNetwork. (2017, 03 20). *Why Alternative Finance will Conquer the $3.3 trillion Market Opportunity?* Tratto da Crowdfund Network:

http://www.thecrowdfundnetwork.com/why-alternative-finance-will-conquer-the-3-3-trillion-market-opportunity/

Danezis, G., & Meiklejhon, S. (2015). Centrally Banked Cryptocurrencies. *IACR Cryptology ePrint Archive*, 502.

Davidson, S., de Filippi, P., & Potts, J. (05/2016). Economics of Blockchain. *Proceedings of Public Choice Conference.* Fort Lauderdale, USA.

Debin, L. (3/2006). *Proof of Work can Work.* School of Informatics, Indiana University.

Deetman, S. (2012, 12 29). *bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.* Tratto da Motherboard: http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

Delivorias, A. (2017). *Crowdfunding in Europe Introduction and state of play.* European Parliamentary Research Service.

Denyer, D. (2016, 10 16). *A literature review in Business and management*. Tratto da Institute for Manufacturing (IfM), University of Cambridge: http://www.ifm.eng.camac.uk/uploads/Research/RCDP/Resources/Working_with_literature_for_Cambridge.pdf

Dienelt, J., & Rizzo, P. (2016). *Understanding Ethereum.* Coindesk.

Dietrich, A., & Amrein, S. (2016). *Crowdfunding Monitoring Switzerland 2016.*

d'Italia, R. (1913). Legge notarile. *G.U. n. 55, 7 marzo 1913, Serie Generale*.

Do, Q.-T. (2017, 1 3). *Asymmetric Information* . Tratto da World Bank.org: http://siteresources.worldbank.org/DEC/Resources/84797-1114437274304/Asymmetric_Info_Sep2003.pdf

Donkers, W. (2016). *Blockchain: the next game changer in real estate?* Deloitte.

Dorri, A., & al. (9/2016). *Blockchain in Internet of Things: Challenges and Solutions.* Conell University Library.

Dourado, E., & Brito, J. (2014). cryptocurrency. *The New Palgrave Dictionary of Economics*.

Duffield, E., & Hagan, K. (2017, 03 10). *Darkcoin: Peer to Peer CryptoCurrency with Anonymous Blockchain Transactions and an Improved Proofof Work System.* Tratto da dash.org: https://www.dash.org/wp-content/uploads/2014/09/DarkcoinWhitepaper.pdf

Dwork, C., & Naor, M. (08/1992). Pricing via Processing or Combatting Junk Mail. *19th Annual International Cryptology Conference on Advances in Cryptology*, (p. 139-147). Dallas, Texas, USA.

Economides, N. (1993). How to Enhance Market Liquidity. *Global Equity Markets*.

Economist, T. (10/2015). The trust machine. *The economist*, 13.

Edmans, A., & al. (2012). The Real Effects of Financial Markets: The Impact of Prices on Takeovers. *THE JOURNAL OF FINANCE • VOL. LXVII, NO. 3*, 933-971.

Ellman, M., & Hurkens, S. (10/2016). *Optimal Crowdfunding Design.* Barcelona GSE Working Paper Series.

Ennis, P. (2016, 12 03). *The Four Types of Bitcoin Users*. Tratto da CoinDesk: http://www.coindesk.com/four-types-bitcoin-users/

Erly, P. (2017, 06 07). *How the BlockNotary App and EULA Work with the Vermont Blockchain Law*. Tratto da CoinTelegraph: https://cointelegraph.com/press-releases/vermonts-new-blockchain-data-authentication-law

ESMA. (02/2017). *The Distributed Ledger Technology Applied to Securities Markets.* ESMA.

ESMA. (06/2016). *Discussion Paper The Distributed Ledger Technology Applied to Securities Markets.* ESMA.

ESMA. (2017, 03 20). *Investment-based crowdfunding.* Tratto da europa.eu: https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1378_opinion_on_investment-based_crowdfunding.pdf

ESMA. (2017). *The Distributed Ledger Technology Applied to Securities Markets.*

Evans, D., & Schmalensee, R. (2010). Failure to Launch: Critical Mass in Platform Businesses. *Review of Network Economics Volume 9, Issue 4*.

Faggart, E. (2017, 03 14). *The Top 5 Cryptocurrency Failures of All Time*. Tratto da http://bitcoinist.com: http://bitcoinist.com/cryptocurrency-failures-all-time/

Fiedler, S., & Horsch, A. (2014). Crowdinvesting als Finanzierungsalternative.

Firoozi, F., & Al. (2017). Information Asymmetry and Adverse Wealth Effects of Crowdfunding. *he Journal of Entrepreneurial Finance: Vol. 18: Iss. 1*.

Folger, J. (2017, 04 19). *The High Cost of Crowdfunding* . Tratto da Investopedia: http://www.investopedia.com/articles/personal-finance/031416/high-cost-crowdfunding.asp

Freedman, D. M. (2017, 04 13). *SAFE: Simple Agreement for Future Equity*. Tratto da financialpoise.com: https://www.financialpoise.com/columns/crowdfunding-for-investors/safe-simple-agreement-for-future-equity/

Freedman, D., & Nutting, M. (2015). *EQUITY CROWDFUNDING FOR INVESTORS.*

Gabison, G. (2015). *Understanding Crowdfunding and its Regulations.* Joint Research Centre Institute for Prospective Technological Studies.

Gandal, N., & Halaburda, H. (2016). Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *doi:10.3390/g7030016*.

Gilbert, S., & Lynch, N. (2002). Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services. *Acm Sigact News 33.2*, 51-59.

Giudici, G., & al. (2016). *1° Report italiano sul CrowdInvesting.* Milano: Politecnico di Milano.

Godet, M. (2004). SCENARIOS AND STRATEGIES A TOOLBOX FOR PROBLEM SOLVING. *LIPSOR Working Papers*.

Grant, T. (2016, 09 27). *R3 & Distributed Ledger Technology.* Tratto da whitehouse.gov: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/10.40%20D%20Grant.pdf

Grigg, I. (2017, 02 19). *The Ricardian Contract* . Tratto da http://iang.org: http://iang.org/papers/ricardian_contract.html#ref_11

Groarke, D. (8/2016). *Blockchain in the Energy and Utilities Industry,.* Indigo Advisory Group.

Guan, L. (2016). *A Short Literature Review on Reward-based Crowdfunding.* IEEE.

Hackett, R. (2016, 12 18). *Why Goldman Sachs and Santander Are Bailing on R3's Blockchain Group*. Tratto da Fortune: http://fortune.com/2016/11/21/goldman-sachs-r3-blockchain-consortium/

He, D., & al. (2016). *Virtual Currencies and Beyond Initial Considerations.* International Monetary Found.

Hearn, M. (2016, 12 19). *Corda: A distributed ledger*. Tratto da corda.net: https://docs.corda.net/_static/corda-technical-whitepaper.pdf

Hege, U., & Lovo, S. (2017, 03 29). *Sending Signals: The Meaning of Equity vs.Cash* . Tratto da hec.edu: http://www.hec.edu/Knowledge/Finance-Accounting/Financial-Markets/Sending-Signals-The-Meaning-of-Equity-vs.Cash

Heilman, E., & al. (8/2016). Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. *International Conference on Financial Cryptography and Data Security*, (p. 43-60).

Hemer, J. (2011). *A Snapshot on Crowdfunding.* Fraunhofer Institute for Systems and Innovation Research ISI.

Heminway, J. M. (2016). *Securities Crowdfunding and Investor Protection.*

Heyek, F. (1974). *Denationalization of Money: The Argument Refined.* London: THE INSTITUTE OF ECONOMIC AFFAIRS.

Higgins, S. (2017, 06 07). *Arizona Governor Signs Blockchain Bill Into Law*. Tratto da CoinDesk: http://www.coindesk.com/arizona-governor-signs-blockchain-bill-law/

Hill, S., & Houde, C. (1997). *What do Prototypes Prototype?* Amsterdam: Apple Computer, Inc.

Hillbom, E., & Tillstrom, T. (02/2016). *Application of smart contract and smart property utilizing blockchains.* Chalmers University of Technology.

Hornuf, L., & Schwienbacher, A. (2014). CROWDINVESTING – ANGEL INVESTING FOR THE MASSES? In H. Landstrom, *Handbook of Research on Venture Capital: Volume 3. Business Angels.*

IBM. (2016, 12 18). *IBM Blockchain*. Tratto da IBM bluemix: https://console.ng.bluemix.net/docs/services/blockchain/index.html?pos=2

Investopedia. (2016, 12 10). *Letter Of Credit*. Tratto da Investopedia: http://www.investopedia.com/terms/l/letterofcredit.asp

Investopedia. (2016, 12 10). *Trade finance definition*. Tratto da Investopedia: http://www.investopedia.com/terms/t/tradefinance.asp

Investopedia. (2017, 04 08). *Corporate Governance*. Tratto da Investopedia: http://www.investopedia.com/terms/c/corporategovernance.asp

Isle, B. (2017, 03 14). *Top Three Failed Cryptocurrency and Blockchain ICOs*. Tratto da bitcoinisle.com: http://www.bitcoinisle.com/2016/12/12/top-three-failed-cryptocurrency-and-blockchain-icos/

Jevos Stanley, W. (1875). *Money and the Mechanism of Exchange* .

Jones, A. (2016, 12 19). *When is a blockchain not a blockchain? When it's Corda*. Tratto da Altus.co.uk: https://www.altus.co.uk/consulting/blog/archive/when-is-a-blockchain-not-a-blockchain-when-its-corda/

Jones, C., & Sirri, E. (03/2010). *Examining the Main Street Benefits of our Modern Financial Markets.* U.S. Chamber of Commerce.

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Scandinavian journal of social theory*, 1-14.

Kerner, S. M. (2016, 12 17). *Hyperledger Blockchain Project Is Not About Bitcoin*. Tratto da http://www.eweek.com/: http://www.eweek.com/cloud/hyperledger-blockchain-project-is-not-about-bitcoin.html

Kosten, D. (2017, 1 3). *Crypto-Socialism- What's next.* Tratto da The Bitcoin News: http://thebitcoinnews.com/wp-content/uploads/2015/11/Crypto-Socialism-What-Is-Next.pdf

Krawiec, R., & al. (8/2016). *Blockchain: Opportunities for Health Care.* Deloitte Development LLC.

Kshemkalyani, A., & Singhal, M. (2008). Consensus and agreement algorithms. In *Distributed Computing* (p. 510-531). Cambridge: Cambridge University Press.

Lambert, & Schwienbacher. (2010). *An empirical analysis of crowdfunding.*

Lambert, T., & Schwienbacher. (2010). *An Empirical Analysis of Crowdfunding*.

Lamport, L., & al. (06/1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3,* 382-401.

Lamport, L., Shostak, R., & Pease, M. (1982). *The Byzantine Generals Problem.* Microsoft Research.

Lazanis, R. (2016, 12 04). *How Technology Behind Bitcoin Could Transform Accounting as We Know It*. Tratto da www.techvibes.com: https://techvibes.com/2015/01/22/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22

Le Hors, A. J. (2016, 12 17). *Hyperledger Whitepaper.* Tratto da http://www.the-blockchain.com/: http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf

Lehmann, R., & al. (08/2013). *Managing Export Risks.* PostFinance AG and Switzerland Global Enterprise.

Leiba, O. (2016, 11 30). *Colored-Coins-Protocol-Specification*. Tratto da GitHub: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Introduction

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal, Vol. 26 Issue: 2*, 110-139.

Lenstra, A. K., & Wesolowski, B. (5/2016). Trust, and public entropy: a unicorn hunt. *Random Bit Generation Workshop 2016*. National Institute of Standard Technologies.

Ley, A., & Weaven, S. (2011). Exploring agency dynamics of crowdfunding in start-up capital financing. . *Academy of Entrepreneurship Journal* .

Luu, L., & all. (10/2016). Making Smart Contracts Smarter. *CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* , 254-269.

M. J. Fischer, N. A. (1985). Impossibility of Distributed Consensus with One Faulty. *Journal of the ACM, 32,* 374–382.

Manju, H. (2016, 12 10). *Supply chain finance- Emerging trends in trade finance*. Tratto da linkedin.com: https://www.linkedin.com/pulse/supply-chain-finance-emerging-trends-trade-manju-hc

Mariotti, S. (2015). *Notes from the course of "Economia dei sistemi industriali"*. Milan.

McConaghy, T. (2017, 04 15). *The DCS Triangle*. Tratto da bigchaindb.com: https://blog.bigchaindb.com/the-dcs-triangle-5ce0e9e0f1dc

McKenny, A., & al. (02/2017). How Should Crowdfunding Research Evolve? A Survey of the Entrepreneurship Theory and Practice Editorial Board. *Entrepreneurship Theory and Practice*.

Melnychenko, O., & Hartinger, R. (2016). ROLE OF BLOCKCHAIN TECHNOLOGY IN ACCOUNTING AND AUDITING. *International Collection of scientific proceedings «European Cooperation», [S.l.], v. 7, n. 14*, 9-19.

Mills, D., & al. (2016). *Distributed ledger technology in payments, clearing, and settlement.* FED.

Moffatt, M. (2017, 04 03). *Definition of Liquidity*. Tratto da thoughtco.com: https://www.thoughtco.com/definition-of-liquidity-1146123

Morgan, M. (01/2016). Blockchain Breakout Session. *Digital money symposium.*

Morini, M. (3/2016). *From "Blockchain hype" to a real business case for Financial Markets.* Bocconi University and Banca IMI.

Morris, E. (10/2016). *Fintech analyst report Part2 Bitcoin/Blockchain.* PitchBook Data, Inc.

Mullins, D. (2017, 05 23). *Does the Capital Asset Pricing Model Work?* Tratto da Harward Business Review : https://hbr.org/1982/01/does-the-capital-asset-pricing-model-work

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* bitcoin.org.

Nassr, I., & Wehinger, G. (2015). Unlocking SME finance through market-based debt: Securitisation, private placements and bonds. *OECD Journal: Financial Market Trends* .

Nickolas, S. (2017, 1 3). *What is the difference between moral hazard and adverse selection?* Tratto da investopedia.com: http://www.investopedia.com/ask/answers/042415/what-difference-between-moral-hazard-and-adverse-selection.asp

Niepmann, F., & Schmidt-Eisenlohr, T. (2015). International Trade Risk and the Role of Banks. *International Finance Discussion Papers 1151*.

Noether, S. (2015). RING CONFIDENTIAL TRANSACTIONS. *Cryptology ePrint Archive, Report 2015/1098*.

O'Dwyer, K., & Malone, D. (2014). Bitcoin Mining and its Energy Footprint. *Irish Signals & Systems Conference 2014*.

O'Ham, T. (2012, 12 29). *Bitcoin Hash Rate exceeds 1 EH/s For the First Time.* Tratto da bitcoinist.com: http://bitcoinist.com/bitcoin-hash-rate-exceeds-1-ehs-for-the-first-time/

Park, Y. S. (2006). *The Inefficiencies of Cross-Border Payments: How Current Forces Are Shaping the Future.*

Pass, R., & al. (08/2016). Analysis of the Blockchain Protocol in Asynchronous Networks. *Cryptography Reunion.*

Patel, D. (2008). Overview of information security and cryptography. In *Information security: theory and practice.* New Delhi.

Peters, G., & Panayi, E. (2016). Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. *Banking Beyond Banks and Money*, pp 239-278.

Phantomcircuit. (2016, 12 30). *Block size limit controversy*. Tratto da BitcoinWiki: https://en.bitcoin.it/wiki/Block_size_limit_controversy

Poelstra, A. (3/2015). *On Stake and Consensus.* Satoshi Nakamoto Institute.

Polasik, M., & al. (10/2014). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. *Available at SSRN: https://ssrn.com/abstract=2516754*.

Poon, J., & Dryja, T. (2016, 12 31). *The Bitcoin Lightning Network Scalable Of-chain Istant Payments.* Tratto da lightning.network: https://lightning.network/lightning-network-paper.pdf

Probst, L., & al. (04/2016). *Blockchain applications & services.* Business Innovation Observatory.

QingChun, S., & Yu, J. (10/2015). *Research on Anonymization and De-anonymization in the Bitcoin System.* Cornell University Library.

Quisquater, J.-J., & all, &. (1989). How to Explain Zero-Knowledge Protocols to Your Children. *CRYPTO '89 Proceedings on Advances in cryptology* , (p. 628-631).

R3Cev. (2017, 01 21). *R3 Cev Response to ESMA.* Tratto da ESMA: https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets#TODO

Rao, M. (2012). FUNDAMENTALS OF ACCOUNTING FOR CPT. PHI Learning Private Limited.

Rapoport, P., & al. (11/2014). *professionals, The Ripple Protocol: A deep dive for Financial.* San Francisco: Ripple labs Inc.

Ream, J., & al. (2016). *Upgrading blockchains: Smart contract use cases in industry.* Deloitte university Press.

Ream, J., & al. (2016). *Upgrading blockchains: Smart contract use cases in industry.* Deloitte University Press.

Redman, J. (2016, 12 19). *R3CEV Unveils Corda, But 'Is Not Building a Blockchain'.* Tratto da Bitcoin.com: https://news.bitcoin.com/r3cev-corda-is-not-building-a-blockchain/

Redman, J. (2017, 03 10). *Meet the Top 3 Coins in the Cryptocurrency Anonymity Race*. Tratto da Bitcoin.com: https://news.bitcoin.com/meet-top-3-coins-cryptocurrency-anonymity-race/

Reid, F., & Harrigan, M. (5/2012). *An Analysis of Anonymity in the Bitcoin System.* Cornell library University.

Reply. (2017, 01 21). *Reply response to ESMA.* Tratto da ESMA: https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets#TODO

Reuben Bramanathan, a. (2017, 05 24). *Introducing the Blockchain Token Securities Law Framework.* Tratto da coinbase.com: https://blog.coinbase.com/2016-12-07-blockchain-token-securities-law-a66ef03c383f

Ripple. (2016). *The Cost-Cutting Case for Banks.*

Rivest, R. L., & al. (2001). How to leak a secret. *Advances in Cryptology???ASIACRYPT 2001*, 552-565.

Robock, Z. (2014). The Risk of Money Laundering Through Crowdfunding: A Funding Portal's Guide to Compliance and Crime Fighting. *Michigan Business & Entrepreneurial Law Review*.

Russo, D., & Mooney, J. (2012). *Principles for Financial Market Infrastructures* . BIS.

Samman, G., & Jew, B. (11/2016). *BLOCKCHAIN AND SHARED LEDGERS THE NEW AGE OF THE CONSORTIUM.* Gilbert and Tobin.

Sandmo, A. (2017, 1 7). *Pigouvian taxes*. Tratto da Dictionaryofeconomics.com: http://www.dictionaryofeconomics.com/article?id=pde2008_P000351

Saunders, M., & al. (2009). *Research methods for business students.*

Saunders, S. G. (2009). Scenario planning: a collage construction approach. *Foresight, Vol. 11 Issue: 2*, 19-28.

Schneider, J., & al. (5/2016). *Blockchain, putting theory into practice.* The Goldman Sachs Group Inc.

Schoemaker, P. (1995). *Scenario planning: a tool for strategic thinking.* Massachussetts Institute of Technology.

Schrijvers, O., & al. (2016). Incentive Compatibility of Bitcoin Mining Pool Reward Functions. Tratto da emanticscholar.org.

Schwartz, A. (2016). The Digital Shareholder. *MINNESOTA LAW REVIEW.*

Schwartz, D., & al. (2014). *The Ripple Protocol Consensus Algorithm.* Ripple Labs Inc.

Shi, R. P. (2016). Hybrid Consensus: Efficient Consensus in the Permissionless Model. *Cryptology ePrint Archive, Report 2016/917*.

Silverberg, K. (2016, 12 29). *Banking on the Blockchain Reengineering the Financial Architecture.* Tratto da Institute of International Finance: http://www.iif.com

Singapore, M. A. (2015). *FAcilitating securities-based crowdfunding* . Monetary Authority of Singapore.

Smith, M. (2013). *Luca Pacioli: The Father of Accounting.* Murray State University.

Snow, P., & al. (2017). *Factom Business Processes Secured by Immutable Audit Trails on the Blockchain.*

Stark, J. (2017, 02 18). *Making Sense of Blockchain Smart Contracts.* Tratto da CoinDesk: http://www.coindesk.com/making-sense-smart-contracts/

Steinberg, S. (2012). *The Crowdfunding Bible: how to raise money for any start-up, videogame or project.* Jon Kimmich.

Steinberg, S. (2012). The crowdfunding Bible: how to raise money for any startup, videogame, or project.

Stephanie, L., & Wnag, C. (09/2014). *Bitcoin as Money?* Boston: FED Boston.

Stephanie, M., & Weatherston, J. (2014). *The Benefits of Online Crowdfunding for Fund-Seeking Business Ventures.*

Stewart, I. (5/2014). *Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn.* www.slimcoin.org.

Sukumar, N. (2017, 01 21). *World federation of exchanges for ESMA.* Tratto da ESMA: https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets#TODO

Swedbank. (2016, 12 10). *Documentary credits, collections and guarantees*. Tratto da Swedbank: https://www.swedbank.ee/static/pdf/business/finance/trade/Hansa_A4_dokmaksed_eng_UUS.pdf

Symbiont. (2017, 01 15). *Distributed Ledgers vs. Centralized Databases.* Tratto da symbiont.io: https://symbiont.io/uncategorized/distributed-ledgers-vs-centralized-databases/

Szabo, N. (09/1997). *Formalizing and Securing Relationships on Public Networks.* First Monday (http://firstmonday.org/index).

Szmukler, D. (2016). *Applying cryptotechnologies to Trade Finance.* Paris: Euro Banking Association.

Teo, E. (2015). Emergence, Growth, and Sustainability of Bitcoin: The Network Economics Perspective. In D. Lee, *HANDBOOK OF digital currencies* (p. 191-200). Elsevier.

Terry, H., & al. (2015). *The Future of Finance: The Socialization of Finance.* Goldman Sachs Global Investment Research.

Thorsteinson, P. (8/2003). Asymmetric Cryptography. In Thorsteinson, *.NET Security and Cryptography* (p. 99). Prentice Hall.

Tomczak, A. a. (2013). A conceptualized investment model of crowdfunding. *Venture Capital: An International Journal of Entrepreneurial Finance*.

trends, G. (2017, 03 14). *google trends*. Tratto da Google trends : https://trends.google.it/trends/explore?q=blockchain

Tschorsch, F., & Scheuermann, B. (2016). A Technical Survey on Decentralized Digital Currencies. In *IEEE Communications Surveys & Tutorials, Vol. 18, No. 3*. IEEE.

UNECE. (2017, 05 04). *Guarantees*. Tratto da unece.org: http://tfig.unece.org/contents/guarantees.htm

Unknown. (2016, 10 29). *Full Nodes*. Tratto da BitcoinWiki: https://en.bitcoin.it/wiki/Full_node

Unknown. (2016, 11 31). *Crypto-Currency Market Capitalizations*. Tratto da Coinmarketcap: https://coinmarketcap.com/

Unknown. (2016, 11 30). *Turing completeness*. Tratto da Wikipedia: https://en.wikipedia.org/wiki/Turing_completeness

Vaizeyv, E., & Hancock, M. (2016). *Distributed Ledger Technology: beyond block chain,.* UK Government Chief Scientific Adviser.

Van de Velde, J., & al. (2016). *Blockchain in Capital Markets.* Oliver Wyman and Euroclear.

Van de Velde, J., & al. (2016). *Blockchain in Capital Markets.* Oliver Wyman and Euroclear.

van der Veer, R., & Gielen, R. (1/2016). *Blockchain: equally disruptive as the advent of the internet.* Kunstmaan.

van Oerle, J., & Lemmens, P. (2016). *Distributed ledger technology for the financial industry*. ROBECO.

van Wirdum, A. (2016, 12 31). *Segregated Witness, Part 2: Why You Should Care About a Nitty-Gritty Technical Trick*. Tratto da Bitcoin Magazine:

https://bitcoinmagazine.com/articles/segregated-witness-part-why-you-should-care-about-a-nitty-gritty-technical-trick-1450827675

Vasek, M., & al. (10/2014). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. *International Conference on Financial Cryptography and Data Security*, (p. 57-71).

Vismara, S., & Signori, A. (2016). Returns on Investments in Equity Crowdfunding.

von Weizsäcker, J. (02/2016). *DRAFT REPORT on virtual currencies.* Committee on Economic and Monetary Affairs.

Voorbraak, K. (2011). *Crowdfunding for Financing New Ventures: Consequences of the Financial Model on Operational Decisions.*

Vukolic, M. (5/2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Open Problems in Network Security*, 122-125.

Wardrop, R., & al. (2016). *Sustaining omentum.*

Wattenhofer, R. (2016). *The Science of the Blockchain.* Inverted Forest Publishing.

Wauters, R. (2017, 03 04). *Kickstarter Launches Another Social Fundraising Platform*. Tratto da techcrunch.com: https://techcrunch.com/2009/04/29/kickstarter-launches-another-social-fundraising-platform/

Wenzlaff, K., & al. (2012). *Definition von Crowdfunding.*

White, M. (11/2016). Socialism and the Blockchain. *Future Internet*.

Williams, G., & al. (2016). *Distributed Ledgers in Payments: Beyond the Bitcoin Hype.* Bain & Co.

Williamson, O. (1973). Markets and hierarchies: some elementary considerations. *American Economic Review 63(2)*, 316-325.

Williamson, O. (1975). Markets and Hierarchies: Analysis and Antitrust Implications.

Williamson, O. (1979). Transaction cost economics: the governance of contractual relations. *Journal of Law and Economics*, 233-261.

Williamson, O. (1983). Credible Commitments: Using Hostages to Support Exchange. *American Economic Review 73(4):*, 519-538.

Wood, G. (2016, 12 30). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.* Tratto da semanticscholar.org:

https://pdfs.semanticscholar.org/79ee/330676c159caf5dce2b2e004a76f966be126.pdf?_ga=1.224149727.574715313.1483020541

Wroldsen, J. (2017). CROWDFUNDING INVESTMENT CONTRACTS. *11 VIRGINIA LAW & BUSINESS REVIEW __ (Spring 2017)*.

Wulf, T., & al. (2010). *A Scenario-based Approach to Strategic Planning – Integrating Planning and Process Perspective of Strategy*. Leipzig Graduate School of Management.

XNotes. (2017, 01 21). *Xnotes answer to ESMA*. Tratto da ESMA: https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets#TODO

Yermack, D. (12/2015). Corporate governance and Blockchain. *NBER WORKING PAPER SERIES*.

Zhang, B., & al. (09/2016). *SUSTAINING MOMENTUM THE 2ND EUROPEAN ALTERNATIVE FINANCE INDUSTRY REPORT*. University of Cambridge .