Ca' Foscari
University
of Venice

Master's Degree Programme in

International Management

Second cycle (D.M.270/2004)

Final Dissertation Thesis

Building Transparency in Supply Chains through Blockchain Innovation - A case study

Supervisor
Ch. Prof. Francesco Zirpoli

Graduand
Susanna Balestra
Matriculation Number 861057

Academic Year
2016 / 2017

INDEX

Building transparency in supply chains through Blockchain innovation - A case study

INTRODUCTION

This elaborate will analyse the impact of Blockchain technology on today globalized supply chains, in particular how it can improve vivid problems like lack of transparency and end-to-end visibility.

Blockchain technology seems to be a disruptive innovation of industry 4.0 with many different and transversal applications, from payment system to insurance sector, anyway one of the most interesting is in the consumer product industry; in fact it seems able to track every passage and every trait of a product along the supply chain.

It is a distributed ledger that allows any participant too see the system of record of all the transactions that happen in the industry, and combines cryptography and a system of incentives to reach consensus between actors; it may decentralize and distribute power from existing authorities and third parties through the use of devices like smart contracts and decentralized apps. This shift may change business models and supply chains; in particular the elaborate analyzes how some mechanisms and features that characterize value transactions in a network, like trust, information sharing and problem solving, may change before and after blockchain, and how Blockchain technology may impose new coordination mechanisms in the network, coherent to its technological infrastructure.

The analysis is based on secondary data; first, the problem of lack of transparency, its consequences and how it is treated by current centralized information technology systems are analyzed in depth. Focus on trust as coordination mechanism in a network, including authors like Granovetter and Uzzi, should highlight the evolution from trust based on cognitive aspects towards a completely new form of "trust" set in the system by the blockchain technology itself. The analysis comprehends a description of Blockchain technology as distributed, open and encrypted ledger of transactions and its main features and applications, furthermore, being blockchain technology an almost new phoenomenon, important growth drivers but also obstacles to mainstream diffusion and adoption are identifiable and analyzed.

Finally, the pilot project that describes how Blockchain technology could track tuna fish from Indonesia to final customers in a transparent way is used as case study to show how blockchain, comparing to traditional methods, would enable better visibility all along the chain and provide completely distributed, reliable and open data to everyone.

CHAPTER 1. LACK OF TRANSPARENCY IN GLOBAL SUPPLY CHAINS

In December 2016 Frank Yiannas, Walmart's vice-president of food safety, went to a Walmart store to start a crucial experiment about supply chain transparency, involving a package of sliced mangoes.

He put the package at the centre of his table and told his team: "Find out where these mangoes came from. I set the timer". It took almost 7 days to give back an answer.

At this point Yiannas, although he was skeptical about the success of blockchain, decided to give it a try and partnered with IBM to run a pilot Project with blockchain tracking the mangoes.

In the project, mango shipments were tracked and digitally registered on blockchain with numeric identifiers from the moment the farmer harvested mangoes; every time they crossed a checkpoint - from the farmer to another supplier, then to the store and so on - their status changed and was tracked in the system.

Some months later Yiannis repeated the same experiment of December at Walmart's annual Shareholder meeting. He entered the numeric identifier in a web portal and it took almost two seconds to have all the information: Mango "Tommy" variety, harvested on 24 April in Mexico, on 25, mangoes were submitted to a special treatment and few days later the shipment entered a U.S. plant where they were sliced and moved to a cold storage facility, and finally they reached the shelves of the Walmart stores.

Two seconds, again, two seconds, to obtain all these specific and dutiful information, compared to almost seven days of the previous experiment.

Lack of transparency and end-to-end visibility in today's supply chains are vivid problems in the food industry but also in the others; this brings serious consequences like foodborne illnesses but also products counterfeiting, supply chain fraud and inefficiencies, problems of trust, environment and workers exploitation and many others.

Finding a system able to track every passage and every trait of a product along the supply chain could help prevent these problems and, as analyzed later in depth, Blockchain could be an optimal solution but obviously there are boundary conditions, costs and other limits to take into account.

1.1 THE CONCEPT OF TRANSPARENCY

In today's economy, supply chains, in particular manufacturing ones, are more and more global and complex, involving a lot of actors all around the world and coordinating different business practices and cultural habits. It's perfectly common for products to be manufactured in China, assembled in Europe and sold in USA. Business transactions are characterized by globalization and internationalization of processes, which bring to an increasing number of transactions parties with different backgrounds.

Before getting to the final consumer, products must cross an extensive network of people working on them; different levels of suppliers, producers, distributors and facilities, etc.

However there is still too poor knowledge of when, where and how products have been created and for some products, in particular food, drugs, diamonds, luxury watches and bags, fine art and so on, there is a strong demand for knowledge and transparency.

Without effective transparency, the supply chain has a potential and dangerous blind spot that risks to expose the management to legal, financial and especially reputational risks.

As Hofstede stressed out (2003), finding an efficient way of exchanging information in today's complex environment "is the key to improve value chain performance and competitiveness". Said simply, transparency could enable companies to be more responsive to events along the chain - facing accidents, refreshing forecasting, etc. - and actors to be more aware about purchased products.

To focus on this problem at best, the first thing to do is making order in the terminology:

- *Supply chain transparency:* is *"the extent to which all the netchain's stakeholders have a shared understanding of, and access to, the product-related information that they request, without loss, noise, delay and distortion." (Hofstede, 2003, p. 18).*
  It refers to all the stakeholders involved in the network created by supply chains; it is a fundamental capability concerning not only the exchange of information regarding products, but it's more about the clear communication to everyone for the correct functioning of the supply chain.

- *Supply chain visibility:* refers to the ability of a firm in a supply chain to see and to know what's happening downstream and upstream, it has a direct impact on traceability.
- *Supply chain traceability:* is *"the ability to trace the history, application or location of that which is under consideration". (ISO 9000:2000).* It can be considered as a synonymous of visibility and transparency but a clarification is necessary; to trace means "sending information down the chain from producer to customer", while to track "is sending information up from customers to producers" (Hofstede, 2003).

  The key point is that tracking and tracing are characterized by flow of information, while in transparency information exist, are "here", potentially available to everyone.

According to the scholar Hofstede (2003), there are three levels of transparency:

- History transparency: is focused on past information, aimed at tracing back the provenance of products in the supply chains. It can be considered as the synonymous of supply chain traceability.
- Operations transparency: is focused on present issues, allows sharing information about day by day business operations, enabling collaborative planning of daily activities.
- Strategy transparency: is focused on future challenges, requires sharing aimed at a long-term strategic perspective.

Considering the aim of this thesis, lack of transparency intended in the strict sense of sharing not information in the network is referred especially to the two first levels of transparency, where a new system organized around blockchain technology could bring many benefits, described later in the essay.

As illustrated in Figure 1, Theuvsen (2003, 2004) elaborated a theoretical framework in which he identified two principal kinds of determinants of transparency in supply chain: structural and behavioral factors. Structural factors include supply chain's, product's

and transactions' characteristics, while behavioral factors include cultural aspects, trust, social embeddedness, partner's attitude and the quality of business relationships.

To describe the phenomenon in an exhaustive way, determinants of transparency can be described as follows:

- *Supply chain's characteristics:* supply chain is organized in input-output relations - called interdependencies - between partners, that enable exchanges of value - in form of money, goods but also information. Every relation constitutes a point in which information are transmitted from one to the other parties, so inevitably the more are the interdependencies, the more difficult is the implementation of transparency.

  Interdependencies are very differentiated, depending on other characteristics like *the length of supply chain, number of transaction partners, frequency and extent* (volume of value exchanged) *of transactions* and *geographical distance between partners.* Today, with globalization and internationalization of production, these variables are acquiring more relevance; in fact supply chains are geographically distributed over the whole global surface, the length of the chain and the number of transaction partners is increasing, just think that only the suppliers are organized on different levels, and they are geographically dispersed. Obviously this scenario causes a necessary change in the way transparency is achieved.
- *Product characteristics:* transparency is relevant for some categories of products more than others. Considering manufacturing products, food, pharmaceutical, luxury industries are some of the most impacted because they are based on attributes like authenticity, genuineness, and adherence to quality standards that should be certified.
- *Transaction characteristics:* include aspects like complexity and uncertainty, transaction-specific investments, governance structure and explicitness of information needed. Complexity and uncertainty should have a positive impact because actors should be more encouraged to receive more information and consequently to share more. Considering governance structure, where governance is based on high collaboration and integration, there is higher

transparency; while where governance is based on power asymmetries and opportunistic behaviour, transparency is negatively affected. Finally explicit information is easier to find and share than implicit information, the more explicit it is, the less is need of interpretation. Furthermore high relevance of information should affect positively the partners' purpose to be more transparent.

- *Culture and social embeddedness:* similar cultural background improves transparency between partners, because they are expected to have a "shared understanding of information" (Hofstede, 2003). As highlighted in next paragraphs, social embeddedness creates high levels of trust, without need of third parties, so it's fundamental to prevent opportunistic behaviour and power asymmetries but it's also difficult to implement, furthermore trust is a concept deeply impacted by blockchain technology. Networks organized around social contacts and communication through physical contact are subjected to trust-building processes and are more propense to exchange information.

  Anyway "hidden rules of the game" as well as "declared rules between business partners" (Hofstede et al., 2004) determined by cultural experience and background have a great impact on business relationships.
- *Transactors' behaviour and Relationship quality:* obviously attitudes like abuse of power, willingness to communicate or not, willingness to cooperate influence transparency along the chain. The quality of a business relation depends on attributes like satisfaction, trust and commitment that influence choice of business partners and the management of relations; the higher the quality of the relation, the higher is the transparency.

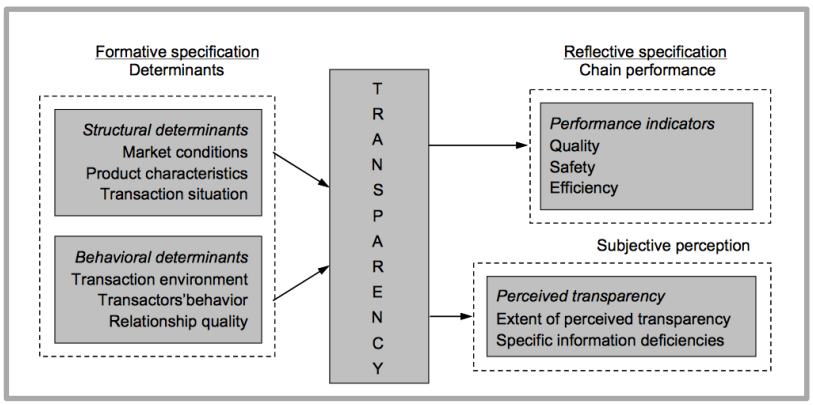

Figure 1: Theoretical framework about definition of transparency (Source: http://www.wageningenacademic.com/doi/pdf/10.3920/JCNS2008.x086)

Beyond these determinants, transparency is also defined by the measuring indicators; one way is measuring transparency through its observable effects, which can take shape of food crisis, illnesses, scandals, etc., described in detail in the next paragraphs. These phenomena measure transparency along the chain, focusing on attributes like safety, quality and efficiency.

Furthermore there is another approach linked to a more subjective dimension and attitude of individuals; named "perceived transparency" by Karg (1990), it is the "feeling of being informed about something and the availability of relevant information as experienced by the individual that makes processes subjectively distinct and clear" (M. Deimel, M. Frentrup and L. Theuvsen, 2008).

After having defined in depth the concept of transparency and the ones correlated, it's evident that it affects customers that could effortlessly know where products come from and how they are produced, likewise other companies and producers could know what happens along the chain. Unfortunately this scenario is not yet the reality, but rather it is an ideal to many. Blockchain technology, as described in the next chapters, proposes as one of its promises enabling global supply chains and networks linked to be more flexible in ensuring transparency to stakeholders connected and to respond quickly to possible accidents and to market demands.

1.2 MANAGING INFORMATION TODAY – Centralized Information Technology Systems

Basically, considering this elaborate, the focus is on information exchanged along the chain as the "lifeblood" of transparency.

First, in the definition of transparency the focus is on "product-related information", in fact considering a product (or a service), there are different kinds of data subject to traceability that today are stored in centralized databases but with blockchain will be available to everyone:

- *Product specific data*: every key information that describes specifically a product. This information is useful to certify some particular features like for example the variety of a food, the carats of a diamond, etc.

- *Location data*: every information concerning the past and the current location of products.
- *Time data:* the date and the time, if it's possible, of every change of location and every transaction. This allows to rebuild the chronological order of transactions.
- *Ownership data:* every information concerning past and current owner of the product. This definitely allows to implement controls of transparency amongst involved parties.
- *Environmental impact data:* every additional information concerning the impact of the product on environment during its life cycle.

Then, today's society has to do with an increasingly changing environment with a higher information production that should be managed by human beings equipped of limited information managing capabilities.
Closing every information gap along the supply chain is fundamental; analyzing ways of managing information today, it's evident that information is stored in fragmented databases. Quite 76% of companies don't have an efficient and automated flow of information across their supply chain for all the needed information.
As highlighted in the case study, data are mainly stored in cloud storage services, located in different places, maintained by centralized servers; so if you want to consult a paper or information stored, you have to pass through an external system of security, often managed by third intermediaries.
Currently the operations of data collection and secure data storage are tasks of non-profit organizations, governmental entities and other third-parties or intermediaries, which use centralized and fragmented databases with limited interoperability. This results in supply chain partners with limited access to overall information.
Obviously, advancements in technology introduced better ways for companies to be better informed about what's happening in the network, the missing ring today is that these technologies without a shared, unique, distributed ledger remain highly disconnected.
For example, current key technologies are Radio-frequency identification (RFID) technology, Barcoding and Tagging; they are in use today and they will be central also in the blockchain application, basically enclosing information, accessible by pointing the camera at the tag. Furthermore many companies start to propose SMS-based surveys

instead of third-parties audit services considering the advantages of real-time data and confidentiality.

Data and information are also registered in billions of excel documents, paper documents and transmitted through emails, spreadsheets, certificates; a lot of paperworks resulting in a transfer which sometimes could be as slow as the transfer of products or also slower.

Also the organizations that promoted visibility and transparency are unable to see behind every corner, particularly when goods are in transit. Infact transport and transfer of products remain highly dependent on this relevant number of paperworks that is never digitized. Sending a shipment of products overseas produces hundreds of paper documents from the actors along the supply chain; then these documents must be stamped and signed, and often they should be delivered in their original version to the next receiver because people don't trust always scanned versions.

Moreover, in the current system data can be easily deleted or modified without any trace of it, while with blockchain technology data are permanently recorded in the ledger without any possibility of changing or modify them without consequences on the previous blocks.

In recent years institutions like European Union or United States imposed new legislations in the field of transparency (e.g. Regulation (EC) 178/2002). Consequently many supply chains are using Sustainability and ethical Standards or International certifications such as Fairtrade, Forest Stewardship Council, emission standards or anti-counterfeiting certifications, which in the past represented a great step forward in the field of transparency, but in reality they are only a logo or an image on products; once consumers see the logo and want to verify it, they are not able and are forced to accept it.

But recent scandals involving food and other industries threatened the credibility of these standards; for example in 2015 Volkswagen made its cars seem less polluting than they were, cheating in emission tests, but the US Environmental Protection Agency discovered that quite 400.000 diesel cars were emitting 40 times more dangerous emissions than expected and allowed, so at that point Volkswagen has admitted the fraud involving 11 millions of cars worldwide. Obviously this had terrible consequences in terms of trust of consumers and brand reputation.

The situation is also worsened by the spread of certification systems from highly corrupted regions of the world.

This kind of centralized information technology system has been the most practical until now, but nowadays it's evident that no single or few organizations succeed in managing data efficiently and this produces an inevitable weakness and bias in the whole supply chain.

The most relevant issue of having a centralized system is admitting a single point of failure in the system, which leaves the supply chains vulnerable to failure in case of hacking or corruption, for example. In the past some scandals showed that a tight and costly control is not able to assure the complete data security, leaving the organizations in the network exposed to a potential risk.

As explained later in depth, Blockchain seems to be a disruptive innovation also in the field of information technology, able to transform the today centralized information system in a decentralized information system.

Data managed by Blockchain improve in terms of quality, considering in particular availability and accessibility because it creates an auditable and shared record of the journey of the products, represented by a digital passport, easily accessible to everyone.

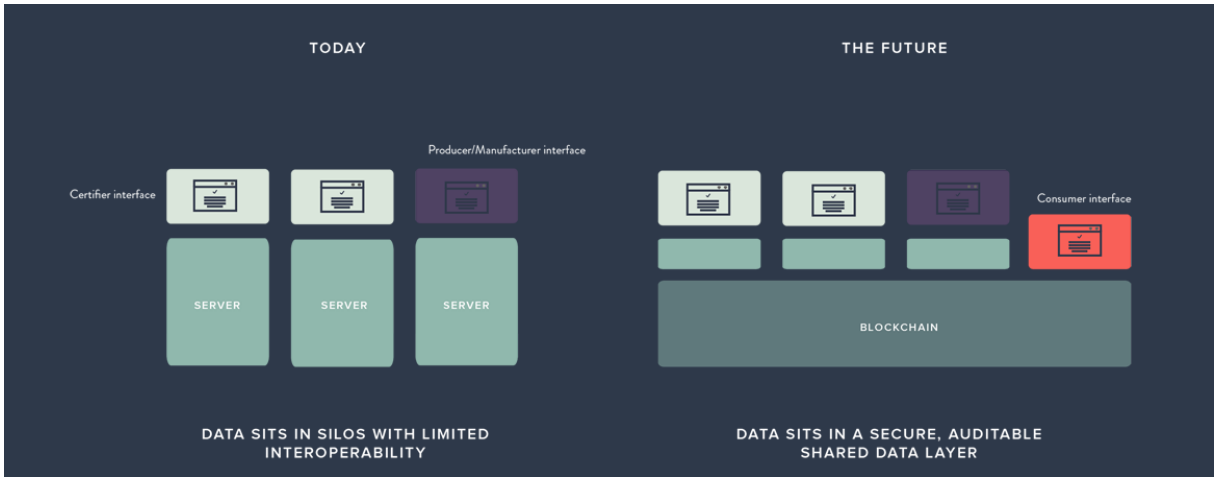

Figure 2 - Centralized/decentralized Information technology system (Source: Provenance white paper)

1.3 DEMAND FOR TRANSPARENCY IS INCREASING - Observable effects

Demand for transparency and visibility along the supply chains is a vivid and really perceived need, both for customers and companies or governments involved, especially considering the real and practical consequences of this problem.
Supply chains are kept secret, limiting the stakeholders to implement measures of protection against social, environmental and healthy problems.

Analyzing examples and episodes, it's possible dividing them into some macro-categories of effects caused by this problem, keeping in mind that they constitute measures of transparency through observable effects:

- ***Workers exploitation and bad work conditions***
  Nestlè, one of the most important food and beverage company, supplies coffee and cocoa from Africa and South America. As in other Multinationals based in the developed world with suppliers located in developing areas, lack of visibility and unawareness of upstream problems in the supply chain is something widely spread. This lack of visibility can result in negative scenarios. Infact, in 2016 Nestlé has been accused by US Supreme Court of exploitation of child labor in the cocoa sourcing from the Ivory Coast. In the same year Nestlè was forced to admit publicly the scarce transparency and control to other stakeholders after a scandal of potential slave labor. Basically Nestlé confirmed that they know very little about the first suppliers of raw materials since they buy them from a large number of plantations, intermediaries and exporters and so it's inevitably possible that unethical practices and slave labor happen within their supply chains. Now Nestlé, like Walmart and other important Multinationals, is working to improve its communications about sustainable sourcing to its customers with projects involving also blockchain.
  Situations like unethical labour conditions or risk of slavery have enhanced the demand for transparency in manufacturing supply chains as an issue of risk prevention and protection for customers but also for workers, especially in the upstream part of supply chain.

Customers are often the most unaware of the various scandals involved in the production. For example, probably iPhone users are unaware of a threat of mass suicide (some effective) at Foxconn factory, one of Apple's major supplier, in Shenzen because of the low pay. And scandals like this have been exploding since more than 20 years, just think of Nike child labour scandal of 1996 in Asia, and obviously with the organization of production in global supply chain they are increasingly spreading.

As explained in detail later, one of the first important project in the field of blockchain for transparency is made by a start-up called Provenance and was developed to track tuna along the supply chain to protect Indonesian fishers from risk of slavery.

- ***Environmental damage and material wastage***

  Connected to unethical labor practices, also material wastages and environmental exploitation are practices typical of global supply chains, in particular when the upstream part is organized in developing countries.

  As it's evident also in the case above, many companies today pursue the ideal of "doing well by doing bad", having bad practices, not considering dangerous consequences like pollution, exploitation, etc. and obviously lack of transparency doesn't enable people to understand the effects and the consequences of a decision about production on the environment. The idea of certifying and attesting that products are aligned with environmental protection standards has become crucial for companies in the last years in front of a more demanding economy, but anyway this has been done always through third parties, like non-profit organizations and associations (e.g. Soil Associations, Fairtrade, etc.), that have managed data, but these procedures remain still not verifiable and not traceable by other actors of the supply chain, first customers.

  In this case supply chain visibility becomes an important enabling factor for the implementation of corporate social responsibility and sustainability initiatives that exhort companies to "do well by doing well", exploiting visibility capabilities to monitor how upstream suppliers and downstream consumers are dealing in terms of employment and work practices, adherence to codes, standards and regulations, sourcing and environmental practices, etc.

In the near future it's possible that also the regulations and the organizations themselves, to fight against exploitation and damage of both environment and people, would require a transparent disclosure of reliable and real information about business operations to make these global problems visible and felt to everyone.

- ***Counterfeit and contaminated products***

  It's recent the case of a salmonella outbreak from Maradol-brand papaya coming from Southern Mexico; the first case was reported in may 2017, and in august other 200 people, in particular young and old people, fell seriously ill, so much that a person also died; the FDA (Food and Drug Administration) worked with the Mexican Authorities to make inspections and controls. Obviously this had terrible consequences for the producers of papayas since importations were stopped to test the products.

  Anyway the central point of this episode is that the cause was determined by the Center of Disease Control (CDC) only once 200 people fell seriously ill; but between May (the first case of Salmonella) and August (the real outbreak) it's evident that no one along the supply chain was able to identify the contamination and to adopt preventive measures to avoid worse consequences because of lack of visibility and transparency towards suppliers.

  IBM is one of the first company to adopt blockchain to improve traceability and it is working in partnership with many companies, first with Walmart, to fight against food contamination because without end-to-end transparency, a timely intervention to prevent outbreaks and illnesses is not possible.

  This is a vivid issue in food industry first, but also for fashion, luxury and healthcare ones; in fact, for example counterfeiting in fashion and diamond industry is a global problem, especially considering document tampering and fraud and, in fact a start-up based in London, Everledger, is largely investing in a project to limit fraud costs and improve traceability of products.

  This problem is the most vivid to customers, more today than in the past, considering problems of allergies and food intolerances that make them more sensible to origin and genuinity of food, in fact quite 30% try to work on this, improving and planning carefully their purchasing decisions.

- ***Inefficiencies along supply chains***

  Obviously this centralized information system based on fragmented and dispersed database and a lot of paperworks causes problems and inefficiencies along the supply chain, exhorting the companies themselves to ask for more transparency, visibility and a better manage of data.

  In the today global supply chains, an event, natural or man-made, big or small, on one side of the world can stop production or delivery of a service on the other side and the consequences can be dangerous to companies all along the supply chain, both in terms of financial issues and of reputation, so consequently companies need to be highly reactive and responsive to these events.

  In the UK market quite half companies state that fragmented information result in missed opportunities in terms of sales, in fact without real-time access to reliable data, many companies are unable to supply peaks in demand caused by sales and marketing activities in the past years, making these investments quite without return.

  Also one small error on paper-works can cause a chain of consequences that can result in such delays that risk to spoil shipments or delay payments; some transactions risk to be not registered and certified and become invisible, bottlenecks appear, inventory levels are also affected and reach not-optimal levels, lead times extend.

  For example, shippers receive orders only few days in advance, this make difficult for them to organize shipments and required infrastructure; while if they dispose real-time data, they would forecast and prepare their cargos in advance, let alone to get ready in case of delays, damages or unexpected events.

  Managers and companies are also involved in depth in the consequences of lack of transparency along supply chains due to lack of visibility of data and consequently they, like customers, are the first to ask for more transparency; quite 80% think that if they managed to understand and to detect better the risks involved in the supply chains, they would improve in managing supply chain inventories and coordination, especially operations like inventory control, shipments organization, etc.

  Obviously, as explained later, adopting a new technology poses a risky question and, even if companies perceive this need, they are ready to invest in this

technology and to change their paradigm only if it's possible to demonstrate a positive return after the first years.

Many of the situations above reveal low integrity of the actors involved, intended as the implementation of ethical and good practices and moral commitment to act in a fair way. Reaching high levels of integrity means that firms can get authenticity and trust in front of their stakeholders, in fact firms that pursue integrity are more spurred to open and share knowledge about their practices.

Consequently the market for products of verifiable and traceable origin is growing; after this analysis about major consequences and problems created, it's evident that lack of transparency is a transversal and general problem, affecting first customers but vivid also for the other stakeholders operating in supply chains, that has as extreme consequence loss of trust towards the actors working on products.

Infact, as cited in other parts, there are already pioneering companies, like Provenance, the protagonist of the case study, that started to perceive lack of transparency as a threat for their business and consequently they started to build their competitive advantage on open, transparent supply chains and for now this seems profitable. Just to make an example, tuna supplier John West started using tags with codes on their tuna cans to enable others to trace tuna back to the very first supplier, the fisherman, and only this operation added a greater value to the company's sales.[1]

1.4 TRUSTFUL/TRUSTLESS CULTURE

Trust is a difficult phenomenon to define, anyway it could be defined as "*a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al., 1998, p. 395).*

Basically it has always been described as something fundamental in managing relationships and in maintaining cooperations and business networks, from an economic perspective; it's defined to be a static phenomenon deeply influenced by cognitive, affective, behavioral features combined with personal experience in the past, present and ideas about the future, but also dynamic, in fact it requires time to be

[1] Provenance White Paper stated that only this operation has added £17 millions to the brand's, revealing that this kind of initiative is important not only for final consumers but also for brands and companies.

generated in a proper way, trust brings other trust. Infact initially trust is tested on basic or less important decisions, if the test is successful, the relations make a step forward and become trustful, as in socially emebedded ties. As highlighted by Theuvsen and Frentrup (2008), the dominant and recognizable features of trust building are the voluntariness and the mutuality of the actions between people. Other possible features are "benevolence and fairness, integrity, reliability and credibility, fulfillment of promises and positive reputation".

At this point the spontaneous question is how is trust linked to transparency? Is one fundamental to the other?

For years the most general idea of transparency in a supply chain - exchange and sharing information - has been based on cooperation and collaboration between members of the network; so, when there is trust between parties, transparency is built more easily.

This happens because the concept of trust is closely related to concepts of power derived from opportunistic behaviour and information asymmetries; when people decide to share information to others, obviously they must take into account that the others could use these information in an opportunistic way to gain a competitive advantage.

However this reasoning is contradictory just by definition because "to trust means to accept an objectively incomplete status of information or knowledge as subjectively sufficient" (Apelt, 1999). Consequently tracing back products is an activity signal of no trust because if there is trust, there wouldn't be need to do this.

While, thinking about the contrary, considering if transparency enables trust, it's definitely true; in fact, as explained before, the first aim for which it's important implementing a system ensuring transparency is that stakeholders in the supply chains, customers first, feel strongly the need of trusting the others, the producers, and consequently the products. In fact sharing information about practices will raise the level of trust, especially when people understand the intentions behind the actions and perceived integrity.

Today the modern and globalized supply chains are strongly embedded in the "Trustful" culture; they are used to perceive trust as fundamental for their functioning and think a

circular linkage between trust and transparency exists, basically trust enables other trust, then transparency, and then again trust and so on.

For decades, after the network emerged as alternative between market and hierarchy, social embeddedness, as described later, has been considered an efficient mechanism to ensure trust, based solely on relational and cognitive trust.

But with globalization and digitalization, trust based on actors that know well each other and share cognitive or maybe cultural features can't be efficient in all situations anymore.

As explained by Hofstede (2003) and Theuvsen (2004), as solution to dilemma of trust and transparency, many strategies in the field of supply chain planning are organized around vertical cooperation and integration, in order to limitate power asymmetries and consequent opportunistic behaviour between partners. Many manufacturing supply chains use guidelines and standards on business transactions, in order to standardize the actions of business actors and to facilitate communication in the network.

In particular, to obviate need of trust, today intermediaries play the main role; they are the main protagonists of trustful culture today - non-profit organizations, governmental entities, importers - and have the role of ensuring transparency along the chain. As described before, information and data pass through them that certify to the other stakeholders. Using market-like mechanisms such as monitoring devices and actors, contractual ties, calculativeness is a different vision of governing business transactions along a supply chain. This system seems to create a more trustful environment with reduced risks, but these figures remain not able to totally sort out the trust question.

In fact, as explained also in technical terms later in next sections, blockchain application would be able to build and ensure a sort of "better" trust, it becomes disruptive especially with those intermediaries that work exclusively to "certify" trust.

Anyway what is fundamental to remind all along the essay is that the introduction of blockchain technology in the field of transparency and trust will lead to the passage from a "Trustful" culture of exchanges to a "Trustless" culture of exchanges; "trustless" because, as described later in detail, surely one of the greatest strengths of blockchain technology is the power of introducing trust between two or more parties without the presence of intermediaries or need of cognitive and relational features. Trust is intrinsic and set by the technology rather that the relation between parties, not more extrinsic;

every transaction incorporates integrity and parties can transact value with the expectation that the other actor will behave with integrity. Consequently it's important to point out that trust loses its features of voluntariness and mutuality, because it's set automatically by the system.

Said simply, blockchain technology enables parts involved to exchange value between them without using other actors and certifies, through cryptography, public and private keys and smart contracts, that everyone respects the terms of the transaction.

This technology sets an important "revolution" considering how centralized systems work today; in these systems access and success of transactions are strongly depending on trust, in fact people, business practices, actors are restricted by these rules and there is a widespread belief that the more people enter the network, the bigger is the risk in the network. On the contrary Blockchain works in an alternative way, it "trusts no one but is open to everyone".

An important point to understand is that blockchain seems to work with the most important rule that if you want to succeed you have to play by the rules set by the system itself; so if normally self-interest of people is avoided with systems of control, coordination or trust, here self-interest, intended as self-interest in running the network securely, plays a primary role.

The system proposed and described in detail in the next chapter constitutes a system for transactions without relying on trust; cryptography and a system of keys provide great control over ownership and prevention of the so-called double-spending problem (certify money spent in order to not spend them again).

Throughout a special mechanism, network is able to maintain its Peer-to-Peer architecture with an "unstructured simplicity", robust and safe from external attacks; actors involved work together with coordination. Thanks to the consensus mechanism, they are able to express acceptance of new transactions, reject invalid ones, establish needed rules and change incentives.

Basically every event that takes place along the supply chain is registered on a permanent record, visible in every moment to everyone and overall verifiable. In supply chain's environment this is a step forward also in terms of reputation; having an available permanent distributed ledger means that everyone involved in the network can see everything about past transactions with the others. Information concerning one person is collected all together and perfectly accessible, every actor in the real business

world correspond to a “personas” on blockchain, once profiles are consulted, people see how efficient that importer could be, how sustainable this manufacturer is and so on. Reputations built on blockchain are based on objective and verifiable data and help organizations to choose partners, to decide whether continuing or stopping a business relation and even to switch business partners midstream if necessary.

A key point to think about it is about the voluntariness in trust, in fact if “transparency is imposed from outside the network, or if the network is in fact institutionally a hierarchy and the leader imposes transparency” (Hofstede, 2003), trust is not anymore “pure” trust; blockchain could “impose” trust automatically, by definition, for its technical features, but can we really define it “trust”? Obviously these aspects are deepened in the next chapters, when it’s explained first how blockchain is able to implement “trustless” transparency in technical terms and then how blockchain implementation changes nature of transactions and role of trust, comparing to the one in embedded ties or to market-like mechanisms.

1.5 THE ROLE OF SOCIAL EMBEDDEDNESS IN NETWORK TRANSACTIONS

As described in the pilot project later, supply chain actors constitute a network whose coordination and trust mechanisms that rule transactions are set by blockchain technology itself, just for how it has been developed from a technical point of view.
As explained in the next chapters, blockchain as a distributed, open, immutable technology that by definition involves a lot of diversified actors interacting within it, with different backgrounds and interests, and, to maintain a level of efficient coordination, these actors should act a positive and collaborative attitude.
A network, as a set of firms that have exclusive and ongoing relationships with each other, has changed and has evolved in the decades; at the end of the elaborate, analyzing the case study about tuna fish, it’s described how the dynamics between actors in the network and how transactions may change with blockchain technology, especially considering the role of trust in economic exchanges; focus on social embeddedness as coordination mechanism in the network used for decades may be used as starting point and comparison element to illustrate how blockchain could disrupt, improve or change features like trust implementation and information sharing.

Following the old and infinite debate whether contractual arrangements cover all the contingencies of economic exchanges or not, assuming a social dimension in networks, resulting in "trust in action", should have the greatest results of cooperation towards innovation and growth, when, according to Granovetter (1985), the network is neither unders-socialized nor over-socialized.

An important phenomenon that has characterized in particular manufacturing supply chains and networks for years is social embeddednes; it is described as "the process by which social relations shape economic action" (Uzzi, 1996). In most cases embeddedness is influenced by personal referrals of people or previous personal ties; in fact many relationships between business partners have been deeply constrained by ongoing social relationships, that influence actors' expectations and chances in ways that the canonical logic of market wouldn't admit. In fact, network theory sustained that embeddedness move actors' motivations away from the simple pursuit of economic profit towards a care of relationships through trust and reciprocity.

It would bring automatically to know better your partners by personal experience or systems of reputation and consequently to build more long-term relationships based often on affective and cognitive closeness.

Then, other experts, like Helper (1990) and Larson (1992), sustained that embeddedness enabled a larger exchange of information than the pure price as in the neoclassical market theory, that involve for example products' know-how, actors' details, etc.

Uzzi (1996) sustained that embedded relationships in the network shared three main features: trust, fine-grained information transfer and joint problem-solving arrangements.

First, trust is considered as the governance mechanism in these embedded relations but it's important to state that this trust is the kind of trust built upon cognitive and relational aspects, in order to make possible a comparison to trust in blockchain network. Researchers sustain that trust, based on cognitive and relational aspects, reduces risk of uncertainty and creates new chances in transacting products. Embeddedness and trust, enabled by cognitive aspects, depend also on criteria like the identity of actors themselves, that becomes critical in assigning a lower or greater value on transaction and may enrich the social capital of transaction partners.

In this specific kind of relationships, trust is a phenomenon for that people are not going to take advantage of other, they are not selfish and relationships with other parties come first; a key issue related to trust is that trust creates an "open architecture" that expects the transaction of services fundamental to survive but difficult to price or specify beforehand, for example when there is a problem in producing a specific good, in a market logic you may expect to not have money, in an embedded tie you may expect to be understood and your actions correctly intended. In this case trust implies extra-efforts, "favors" that are voluntary and reciprocated, and this is particularly interesting because they work autonomously, not as in other coordination mechanisms that use formal devices enforcing reciprocation like formal contracts, fines, intermediaries, etc.

Then, information exchanges include tacit and strategic know-how that determine firms' efficacy and responsiveness to the environment, enabling a form of coordination and learning, different from the neoclassical market theory, based simply on price or quantitative information, in fact long-term collaboration and embedded ties should imply that partners would perform a certain task or work in the intended way by the other party because of the shared know-how and information. Information sharing depends also on identities, in fact identities and social relations can determine the credibility and interpretability of information.

Finally, in dealing with problems, embedded ties act problem solving arrangements, called mechanisms "of voice", that enable firms to solve problems and to improve learning and problem correction, getting direct feedback on problems. Basically in the market mechanism, the strategies in solving problem are "exit" or "stay", if there is a problem, actors think "how it must be". Embeddedness allows a room for innovation in dealing with problems "on the fly", since implies a new combination of ideas and solutions. This mechanism usually intensifies the linkage between actors, just because it exposes them to different dimensions that go beyond economic and business concerns.

The question debated about social embeddedness is that it's all about business and profits, not "friendship"; is it social embeddedness functional to business or not? Many experts, like Uzzi (1996), stated that embeddedness might even equal or overcome the market paradigm in terms of economic opportunities and profit. As described above, points of strength like reduction of monitoring costs, faster decision making, improved organizational learning and adaptation determine not only the success of a firm involved in embedded ties, but of the whole network. Anyway the best solution seems to be

building a network that combines embedded ties with arm's-length ties, since it could ensure the greatest adaptive capability, combining trust, information exchange, joint problem solving of embeddedness with wide access to information in the market and better ability of testing new possible partners. Granovetter (1985) confirmed that the network should be neither too under-socialized nor over-socialized to reach its best efficacy and efficiency.

According to researchers Van Dijk and Theuvsen, building trust through social embeddedness leads to positive effects in term of transparency because reduces the amount of coordination and control requirements in the business network, it constitutes a sort of governance mechanism really focused on social and relational aspects. Furthermore social embeddedness is defined as a "safeguard" against information asymmetries between parties and opportunistic behaviour.

Anyway it is important to clarify that social embeddednes has some limits. First, an excessive embeddedness causes that the exit of a core player is considered a completely unforeseeable event that poses the partners in high risky situations in finding a replacement. Then, organizations that build their competitive advantage at most upon embedded ties risk to fail, if institutional changes preclude and change the conditions to build other ties. And, the so called "overembeddedness" can reduce the level of introduction of innovative ideas and innovative information.

Finally, it's important to state that embeddedness assumes greater importance in situations in which the actors are culturally closed and geographically connected enough to build a trusted relationship, while blockchain could gain a competitive advantage where the actors are connected by the same productive chain but distributed and dispersed throughout the whole world.

CHAPTER 2. THE BLOCKCHAIN TECHNOLOGY

In many occasions in the first chapter, Blockchain technology has been described as a distributed ledger; it's evident that it is a disruptive innovation in many fields, in particular in the field of information technology, but it's time to describe it in depth, starting from the beginning, explaining the technical features and declinations, its applications.

In order to understand the great value of this technology, first, it's important to highlight its distinctive characteristics that would make it an important solution in the field of information technology and supply chain transparency, later in this chapter these characteristics will be described in technical terms.

Before starting, it's fundamental to state that Blockchain technology and cryptocurrencies are deeply interconnected but they are two distinct phoenomena; anyway to understand the functioning of blockchain technology and how it can be applied on supply chains, it's necessary to explain what a cryptocurrency is.

The rules and the technology behind blockchain functioning were developed considering Bitcoin blockchain that has been the very first appearance of blockchain technology, and consequently, in this elaborate, Bitcoin technology is taken as reference because it is the most famous and widespread, anyway people should understand that now there are many other cryptocurrencies and blockchains, sometimes with their different and distinctive peculiarities.

Finally, key technical concepts are explained and described in the most exhaustive and functional way, considering always that the aim of this elaborate is Blockchain innovation as a solution for lack of transparency in modern supply chains.

2.1 BLOCKCHAIN - DEFINITION AND MAIN FEATURES

Blockchain technology first appeared in 2008 as the "backbone" of Bitcoin in the white paper of Satoshi Nakamoto; it was immediately evident for those who read it that a new age of the digital economy was going to start, combining efficiently computer engineering, cryptography and behavioural economics.

As shown in Figure 3, in its most generic definition, Blockchain is a distributed ledger; it's a "chronological chain of blocks" where each of this is destined to contain a "record

of valid network activity since the last block was added to the chain" (Needham & Company, LLC, 2015).

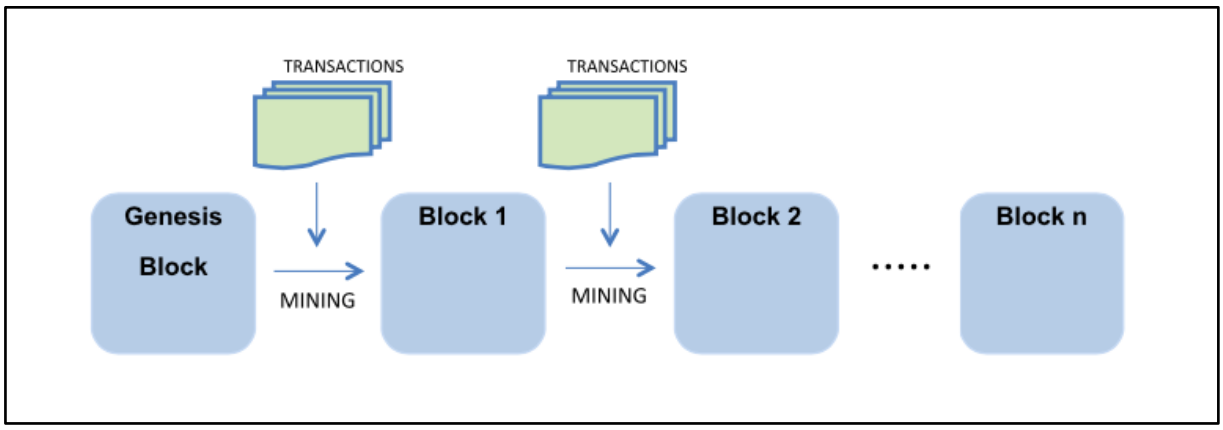

Figure 3 – Blockchain as a chain of blocks containing transactions

Every few minutes, transactions acted in a network are cleared, verified and finally stored and recorded in a block linked to the previous blocks, continuing the chain.

So, to be more specific and to stress better the concept, Blockchain is a "distributed chronological ledger of valid network transactions" that everyone is able to "re-read", everyone is able to add transactions, but what is fundamental is that nobody can change it. Consequently it can be defined as "a complete and immutable history of activity happened within the network".

Basically, this permanent and immutable record can be used to obviate the needs of trust and intermediaries; two or more parties in the network could exchange value (including information) without necessarily trusting or even knowing each other and without relying on middlemen. Particularly when we think about vast and distributed networks created by modern supply chains, Blockchain has a better effect the bigger is the network and the wider is the adoption; it becomes increasingly longer and distributed and consequently more robust and secure.

As said before in the so called "trustless" culture, especially in the field of transparency, this could mean a great step forward, the idea that a value exchange is safe and secure only when certified by third parties is completely dismantled. Not relying on intermediaries to assess trust between parties leads to remove the friction in terms of time, cost and risk.

Infact Blockchain technology presents a *Peer-to-Peer architecture (P2P);* obviously P2P means that all nodes in the network have the same value, without hierarchies inside and without central point of control and centralized service, reaching a decentralized form of control that constitutes a core design principle of this kind of network. All nodes work together and feel the same responsibility of making the network work. Connections between nodes are not regulated by structured and fixed rules but by a random method. Finally the network is completely open, and every node is free of joining or leaving at any time. One of the most relevant examples of Peer-to-Peer network appeared with Napster, a pioneer company whose main scope was sharing files directly between people without a central server.

As described in the next sections, Satoshi Nakamoto in his White paper described the passages to run successfully the network:

1. New transactions are spread to all actors
2. Each node collects all new transactions into a block
3. Each node works to find a difficult Proof-of-work solution for its block
4. When he finds a solution, it broadcasts the block to the other nodes
5. Nodes accept the block only once assessed transactions are valid and unspent
6. Nodes accept the block and start to work on a new block, linked to the previous one

Then, each blockchain (because Blockchain is different depending on the cryptocurrency) shares the same key features, which are:

- ***Decentralized and Distributed Consensus:*** it works running on devices (mainly computers) managed by people, participants distributed all around the world. Decentralized means that it has no single point of control, there is no single entity with the power of controlling the record. Instead of relying on a central authority or on a central database, Blockchain is run and validated by a network of completely independent people (often very dispersed), avoiding the threats of abusing, hacking or just ignoring power. This distribution of power without single point of control expects a peer-to-peer network (P2P) to exist.
  This characteristic makes the system more durable than the centralized systems.

What is fundamental about Blockchain is its ability to reach Distributed Consensus, this is the ability of getting consensus and agreement about the state of transactions from the network without the need of an intermediary certifying it. In this way consensus-based exchanges and actions are smoother and more facilitated, and functioning of blockchain depends a lot on mass collaboration. This decentralized "platform" puts greater power in the hands of end-users.

- ***Public:*** everyone is able to consult it and view it to control transactions and records in every moment because it lays on the network, not relying on a central authority or institution's system. This inevitably makes blockchain appear more transparent and visible, consequently reducing the need of trust.
- ***Immutable:*** transactions and information stored on blockchain remain highly immutable thanks to the fact that the transactions are continuously validated by other people and the previous blocks can not be modified or removed. This is fundamental for this research because it helps business partners to exchange with the highest degree of safety and security that information is real and accurate.
- ***Encrypted and secure:*** as explained later, it is based on encryption built on private and public keys to keep privacy completely intact. This helps maintain the system completely safe and secure because finding both these keys is impossible. Developing Blockchain technology around cryptography makes the system safer from threats like fraud, hacking, identity theft and so on. It marks an important block in the story of financial innovations, in the financial environment new technologies were specialized more in developing technical innovation rather than a secure technology.

The key point, considering the aim of the elaborate, is that working on a network of people without mechanisms of central control and power needs and requires a *Consensus mechanism;* establishing personal trust between members is not possible because people are dispersed and with hidden identities, but the technology is able to ensure trust in transactions and information regardless how the others act.

To achieve consensus, blockchain technology relies on particular mechanisms, explained in the next paragraphs, of which the most important and widespread is called *Proof of*

work, but Tapscott in his book states that other solutions to ensure consensus are going to emerge, like *Proof of stake, Proof of activity, Proof of capacity* and *Proof of storage.*

2.2 BITCOIN AND CRYPTOCURRENCIES

In 2008 Satoshi Nakamoto, a person (or a group of people) called under this pseudonym, wrote a White Paper that established an important change initially in the financial industry but then also in the others, introducing a new "peer-to-peer electronic cash system" called Bitcoin. Basically in that paper Satoshi established some rules that could bring integrity in transactions without relying on trusted third parties. No one ever discovered who Nakamoto really is. His activities, until 2011, are detectable only on the Internet. After then, he left the most important parts of Bitcoin project to Gavin Andresen.

Bitcoin is the first of so called cryptocurrencies, that are currencies based on cryptography and based on a decentralized computer architecture; in fact bitcoin is the name of the protocol, a network and an innovation too.
According to Oxford Dictionary, a cryptocurrency is *"a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank".*
Cryptocurrencies are exchanged on OTC Markets (Over The Counter), which are markets not regulated, working only on digital platforms.
In the world of cryptocurrencies, there are other ones beyond Bitcoin, with different characteristics, Litecoin for example may be directly compared to Bitcoin, while Ether and Ripple are becoming famous for their different applications like Private blockchains and Smart contracts.

As said before, the mechanism behind the correct functioning of the system is called *Consensus mechanism* (described in detail later), elaborated to solve the *Double-spend problem*.
In the classic centralized systems, users are identified with credentials like username and password, stored in central databases and in presence of a third party certifying, while on blockchain, identities are granted by digital signatures combined with a system

of private and public keys. Altering a transaction in a block is quite impossible, because it would mean modify all the past transactions, as they are linked by a chain of digital signatures. Obviously the longer is the blockchain, the more difficult is acting changes.
The double-spend problem consists in the fact that without a central point of control, money risk to be spent twice, while money should be transferred from your account to your friend's account and disappear from the first; it shouldn't be present in both the accounts. Basically this problem is solved by blockchain, where every valid transaction belongs to a block, therefore having a unique and shared timestamp. In this way, obtaining a global consensus of the exact chronological order of all the transactions is guaranteed.

2.3 CRYPTOGRAPHY – PUBLIC AND PRIVATE KEYS

In order to understand Blockchain technology and cryptocurrencies, the concepts of public and private keys are the first to be defined. As they are concepts deeply connected to cryptography and mathematics, in this paragraph they are described in the most functional way considering the aim of the elaborate.

The system works considering keys (private and public), addresses and digital signatures; every transaction needs to be validated by a signature generated by a pair of keys.
There may be several pairs of keys or only one pair per user; every pair is made of one *Private key* and one *Public key.* One of the solutions possibly used is creating different pairs of keys using the same private key but changing public key for every transaction to increase level of privacy.
The public key is fundamental to receive and give Bitcoin, the private key is utilized to "sign" the transactions. Private key must be kept informed only by the owner, while public key could be also shared with others.
The private key is a number generated in a random pseudo mode. It can assume one of the integers ranging from 1 to n where n = 1,158 · 1077 - 1. A possible private key looks like 5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh.
Given the private key (k):

$$K = k \times G.$$

The public key (K) is generated by a mathematical function called *Elliptic Curve Point Multiplication;* K and G are both points on the elliptic curve.

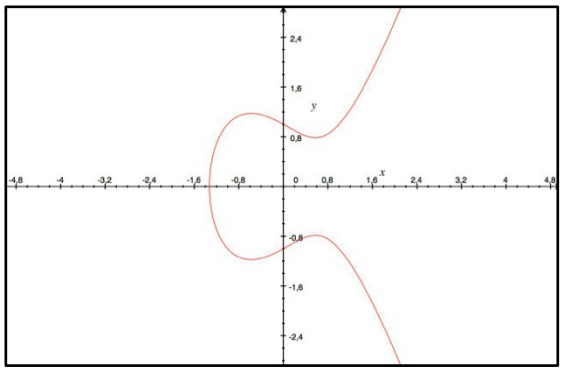

Figure 4 – Elliptic curve that generates the Public key (Source: Mastering Bitcon)

A function of this type is relatively easy to perform directly, while practically impossible to revert, knowing the result. Therefore, even if someone knows your public Key (K) and the function itself (G), he couldn't calculate the private key (k).

Once determined the public key, it's possible to deduce the (Bitcoin) *Address*, fundamental to do the transaction. Basically the address (A) is determined applying a double hash function to the public key (K).
Said simply, every hash function can map data of arbitrary size in data of a fixed and predetermined size. This kind of functions is extensively used in the cryptocurrencies protocols, from generating addresses to linking blocks on the Blockchain.
In fact:

$$A = RIPEMD160(SHA256(K))$$

Where (SHA256(K)) is a hash function developed by National Security Agency (NSA) of US Government, and RIPEMD160 is a European cryptographic algorithm developed in academic environment.
Every address is between 26 and 35 characters long and starts with "1" or "3". Basically it corresponds to IBAN code in the normal financial system.
The relationship between keys and addresses is mathematical and fixed, but the address can be shared with everyone without the risk of revealing the private key because the functions works only in one direction, as evident in figure 5.

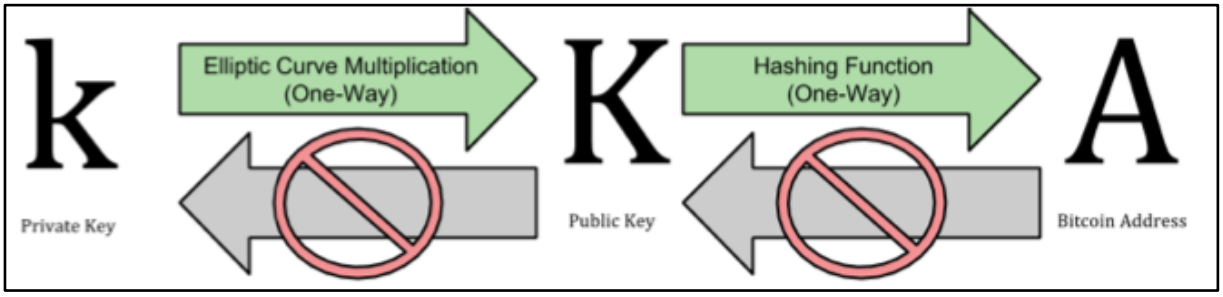

Figure 5 – Relationship between Keys and address (Source: Mastering Bitcoin)

Addresses are presented in encoding ways, in particular "Base58Check" or QR codes; in "Base58Check" the address is converted using a base 58 number that uses uppercase and lowercase letters except some, digits except 0 and not "+" and "-".
The other method is using a normal bidimensional QR Code, which is more convenient because it can be used on phones and on mobile devices facilitating payments transactions between people.

As evident in the figure 6, cryptography and the presence of keys are fundamental to achieve an acceptable level of privacy in the system. In fact in the traditional model, privacy is achieved by limiting access to information about transactions; with blockchain, transactions happen and are announced publicly but keeping keys anonymously allows to maintain privacy in the system.

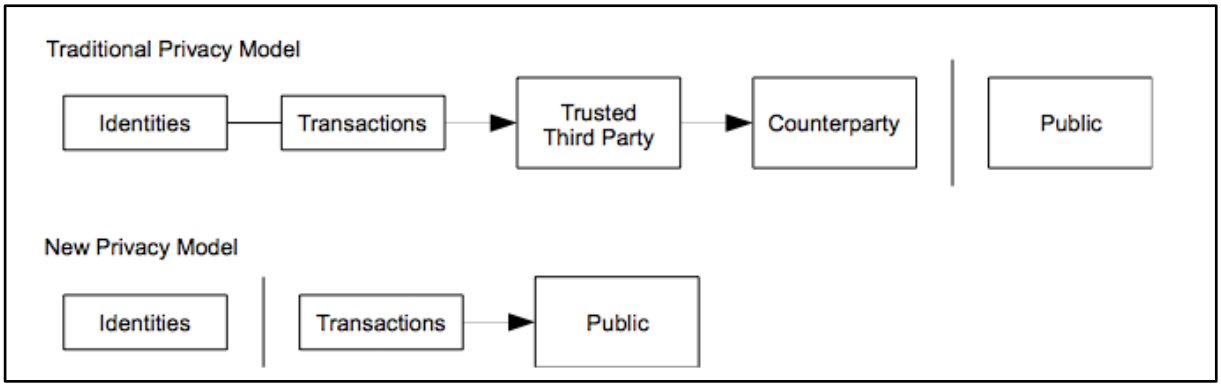

Figure 6 – Difference between traditional and new privacy model (Source: Bitcoin White Paper)

2.4 TRANSACTIONS ON BLOCKCHAIN

But how does blockchain work practically? It is clear that is a chain of blocks and every block contains a number of transactions acted. But how does a transaction work?
In order to give and get "money", the first step is to connect to the network through several softwares or online services that allow these transactions. Infact there are different possible solutions like softwares directly installable on PCs, app to download on devices and online websites accessible with username and password.
To be specific, these are classifiable as full client, that is a software/app that allows the connection to the network and to manage the keys, or lightweight client, that allows only to manage the keys, or finally web client, that is a client directly accessible by browser, and the keys are managed by a remote server.

These solutions allow to manage the so-called *wallet,* the wallet is fundamental to store credentials and to assess the amount of your bitcoins. The credentials are one or more pairs of keys (one public and one private); the keys may be also written on a paper or saved on a pendrive, but obviously these methods have the highest degree of risks like theft, loss or data elimination. To prevent this kind of risks, wallets in turn are protected by a password.
Private keys are all you need to control and transfer your funds, therefore keeping them stored and safe is imperative; possession of keys is everything. Someone who gains access to them can freely manage your coins, and in case of disappearance of the keys, your funds are lost forever.
Both the sender and the receiver must have a valid (Bitcoin) Address because every transaction happens always between the two addresses.

The transaction is similar to *double-entry accounting;* on the left the inputs, on the right the outputs.
Every transaction is charged with a "*transaction fee"*, paid to the validator of transactions, which constitutes a sort of incentive to pursue the activity of validation.
The constituents of an user's balance are not the single coins, but the amounts of unspent previous transactions. Doing a transaction means literally "signing a transaction

that transfers value from a previous transaction over to a new owner identified by a bitcoin address" (Antonopoulos, 2015).

For example, if Alice wants to send 1 bitcoin to Bob and she has previously received 100, she must send 1 to Bob and 99 to herself. With the help of her Bitcoin Wallet, she fills an "electronic check" with the recipient's address, the amount to transfer and a digital signature which certifies that she's in possess of the private key, necessary to move the funds. She could even change the fee she wants to pay, knowing that higher fees lead to her transaction being added to a block sooner.

Once authenticated the identity of the sender, it's important make transactions public and give them a precise and recognized chronological order; until the transaction is not validated, it is defined "unconfirmed" and it finishes in a temporary "pool" of not validated transactions kept by each node in the network, Bob doesn't get paid and so can't send money in turn to someone else.

In fact the transaction rapidly spreads across the peer-to-peer network, getting to the most of the nodes in few seconds. The set of transactions in blocks that are validated by the network is called blockchain. In the next paragraphs the mechanism of validation is described.

2.5 CONSENSUS MECHANISM AND MINING

To achieve consensus, the network uses a mechanism, called *Proof of work*; in order to validate the transactions, people deal with a mathematical problem, which is hard to solve (requires a lot of computational work) but easy to verify, in fact everyone is able to immediately check the solution. Said simply, people in the network have to spend resources (time, work, electricity and computing power) and when they find the solution they receive coins as reward. Everyone in the network knows that the problem is a mathematical problem that doesn't admit shortcuts to be solved, and so when participants see the solution, know that it has required a lot of work and everyone automatically "trusts" that everyone has spent its resources working on it; this is how the concept of trust in the network has changed and transformed.

To run a blockchain successfully, the majority of computing power should be controlled by honest nodes, because the chain will grow in the most honest way and wins over the other competing chains. Nowadays Proof of Work mechanism is the most diffused

consensus mechanism, but researchers are studying and experimenting with other possible solutions; briefly the others mechanisms that in a future are expected to replace Proof of work are for example Proof of stake, that requires to "invest in and to hang on to some store of value" (D. and A. Tapscott, "Blockchain Revolution", pg. 26), without spending work and energy, Proof of capacity and Proof of storage, that require users in the network to give a portion of their hard drive to mining, Proof of activity, etc.

The technical process, based on proof of work mechanism, that validates transaction is called *mining,* which is also fundamental to generate new coins. Said simply, mining is "a competitive game" with the aim of solving a problem and getting the reward.
Mining is fundamental for two purposes:

- Creating and ensuring trust between participants because transactions are validated only when enough computational power is used to do this. More work and computations means more trust in the network.
- Creating new coins per block, every block generates a fixed and decreasing amount of coins.

To stress the concept, Mining activity is able to ensure the consensus in the network without relying on central authorities. Mining is the process that makes this kind of architecture special.

Nodes that are able to run the mining process are called *Miners*, which are able to see the whole blockchain and pursue the mining process.
According to the protocol, a transaction can not considered verified until it's inserted in the Blockchain; miners have literally the role of "gathering up recent transactions, settling them in the form of block of data and repeating this process every ten minutes" *(D. and A. Tapscott, Blockchain Revolution, pg. 25).*

The problem to be solved is a hash algorithm SHA-256, that produces a number 256 bit long, called *hash value.*
Said simply, mining consists in hashing the block header continuously, changing one parameter, until the hash matches a specific target set by the system. The result can't be

determined in advance, nor someone is able to create a procedure that will give a specific hash value. This means that the only way to obtain the result is to try again and again continuously until the value appears by chance.

Just to remind, a hash algorithm is a mathematical function that is very difficult to solve but very easy to verify; just imagine an enormous sudoku puzzle with many rows and columns, it requires a lot of work to be solved, but then it can be easily verified.

The system sets a *target,* a *threshold* and the final goal is to find a value lower that the established target; obviously with decreasing target, the difficulty of the problem is increasing.

To give an example, imagine that you have to throw the dice continuously until you find a number inferior to a set value; the higher is the value, the easier will be finding a correct number.

The number used as an input parameter in this scenario is called *Nonce,* it is fundamental to get different outputs from the hash algorithm.

The final solution is definitely a proof-of-work, as it assesses the work done by people in the network to get the value. For how many necessary computations done to find the solution, it's needed only one computation to verify it.

For example, at the today difficulty level, nodes have to try more and more, billions of times, to find the right nonce able that generates a low enough hash value.

Anyway the difficulty of the problem is set and recalibrated by the system every 2016 blocks in order to maintain the frequency of block validation every ten minutes.

As said before, the idea is to validate a number of transactions, include them in a block and "insert" the block in the blockchain; the Hash function to be solved is referred to the current block.

Whoever tries to solve it and doesn't succeed, has to adjust data and try again, every failed attempt generates an entirely different hash value. This problem solving is continuous (quite 500 000 trillion hashes per second) and on average the solution is found every ten minutes; it's a Poisson process that sometimes requires few minutes sometimes one hour, but on average ten minutes.

The first node able to solve the problem, publishes the solution on the network and the other nodes can verify it very easily. As the block is validated, each node adds it to the current blockchain, extending the height to *n+1* blocks.

Once miners receive the previous block that has been confirmed, they start a process of mining the new block, stating that they have lost the previous round of competition. So they instantly create a new block with transactions "collected on the desk" and start the Proof-of-work calculation for that block.

Whoever solves the problem first, receives new coins as reward. The amount of the reward diminishes with time; initially in 2009 it was set at 50 Bitcoins, every 210.000 blocks (quite 4 years) it is halved, in fact currently it is 12,5 bitcoin. Consequently after 2140 no new bitcoins will be generated with mining because the system will reach the amount fixed by Nakamoto, that is about 21 millions Bitcoin. Another incentive to pursue mining is the earning of fees, as the reward is decreasing and the number of transactions is increasing over time, after 2140 earnings will be all fees. As miners receive fees on transactions as reward, transaction fees could be seen as an incentive to include a specific transaction into the next block.
Incentives are a key point of the system; the idea that the software is programmed to reward those who work on it so that all users can take care of it is one of the milestones of this kind of system.
In fact these incentives have the main role of encouraging nodes to stay honest; whoever has the initial intention of using an enormous amount of computing energy and work to defraud other actors in the network or undermine the whole system, he soon will notice that playing by the rules is in any case better.

2.6 ENERGY CONCERNS

The Mining activity, although it has financial benefits cited above, involves relevant energy costs. In fact Proof-of-work mechanism requires users in the network to expend a lot of computing power, and consequently a lot of electricity.
Initially, to pursue the mining process, people used the Central processor of computers (CPU), now they start using new processors used in the modern PCs, particularly potent in calculation and able to handle 3D graphics. Next step was to create new chips (ASIC, Application Specific Integrated Circuit) reserved for this activity and this kind of calculation.

Stated that Blockchain works successfully because it is decentralized, there is a paradox; in fact while the system is developed considering that no one could be able of having more than 50% of the total computing existing power, today there are big data center that share energy costs and computing energy between actors involved. Furthermore, there are big aggregators of miners, called *Mining Pools,* that, as explained later, constitute a big threat against the decentralization of the system.

In mining pools miners share their hashing power but also the reward among hundred of users; anyway, even if they receive a smaller reward, proportional to the amount of processing power shared with others in the pool, they are very likely to receive it everyday, reducing risk and uncertainty.

Briefly analyzing where current mining pools are, more than 50% of the actual hashing power is controlled by mining pools located in China, where cost of electricity is very low (https://blockchain.info/pools). Obviously this reveals that there is a geographical centralization of hashing power in China that constitutes an important threat to this technology, that was born to boost decentralization and transparency.

The researchers established the cost of total annual production of bitcoin is around 0,74 billion dollars, almost entirely due to electric energy, that in the future may be lowered thanks to renewable sources of energy.

Obviously it's fair to remember and specify that the presence of costs is necessary to avoid fraudulent phenomena but no one could be able to see and forecast the behaviour of people in the network when, for example, the total supply of bitcoin (21 millions) will be available and the only incentive to continue blockchain will be fees on transactions.

2.7 CHARACTERISTICS OF BLOCKS

To understand most of the logic behind Blockchain, it's fundamental to understand some key concepts related to blocks structure.

First, each block is identified by a *hash value*, generated by the SHA256 cryptographic hash algorithm, solved by miners, on the header of the block.

As evident in figure 7, every block has a *Block Header* containing some information, like reference to previous block hash, Timestamp, Difficulty Target and Nonce; in particular the Block Header contains the *Merkle Tree root,* that is a solution used to recap and summarize all the transactions in the block.

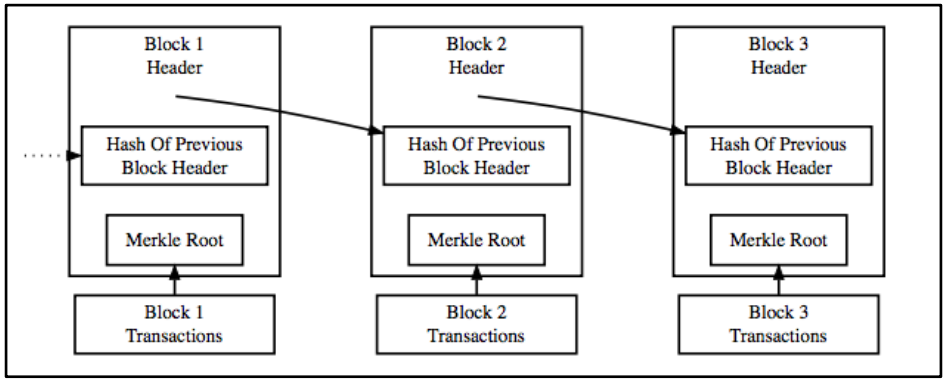

Figure 7 – Structure of blocks (Source: Mastering Bitcoin)

In the block header, there is the "previous block hash" field, which contains the hash value of the previous block, which is called *Parent Block.*

The chain of hash values linking blocks goes back to the very first block, called *Genesis Block.* A block has only one parent, but it can have temporarily multiple children blocks; each of these refers to the same parent block and fills the "previous block hash" field with the same hash value.

The phenomenon that creates more than one child block is called *Fork,* which happens when miners validate simultaneously two blocks. Usually in this case only one block becomes part of the blockchain and the Fork is resolved.

Basically sometimes two nodes spread in the same moment two different blocks, the other nodes receive one or the other and in this case they start working on the first they receive but maintain the other in case it will be chosen as the right one. Once the next Proof-of-work algorithm is solved, the nodes continue on this chain and abandon the other. The rule is that the longest chain is the correct one because it assumes the greatest amount of computing power and work on Proof-of-work mechanism. In this case the fork is called *Soft fork* and, even if it happens almost once a week, it is usually resolved easily within a block, in fact the first block validated after the fork determines the right chain.

But, in very few and rare cases, it can happen that both the blockchains continue independently and in this case it is called *Hard fork*; usually in the case of a hard fork, there are different conceptions about Blockchain development, and one branch continues a blockchain on one side, if the other party doesn't agree, it continues its chain on the other side. Obviously a hard fork generates a split of the currency and the birth of

two different and separate currencies, which start to develop different features for the technology.

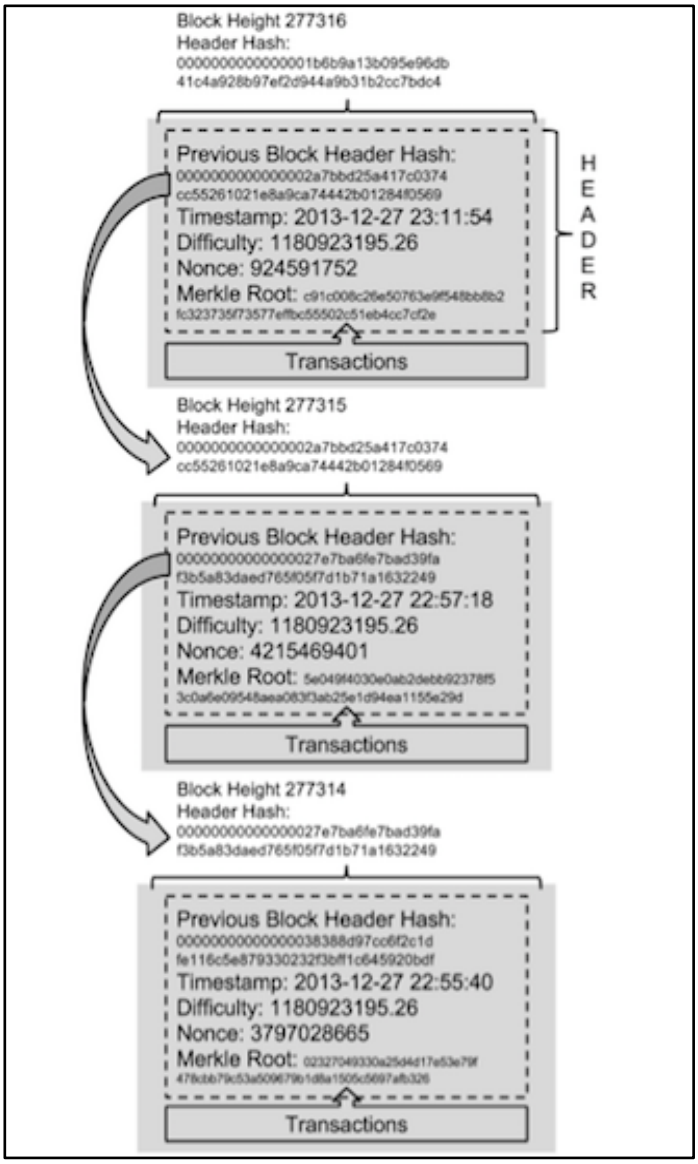

Figure 8 – Features of the blocks (Source: Mastering Bitcoin)

The univocal connection between Parent and Child blocks makes that when a change occurs in parent block's hash it reflects inevitably in the child block's hash. This effect makes that once the *Height* increases, that is a block has many blocks following it, it can't be changed without a recalculation of following blocks. As this recalculation would require enormous computation and work, the longer the chain of blocks is, the more the history is immutable. Therefore old blocks are less and less likely to be corrupted; as a

common standard, transactions contained in blocks with a height higher tran six are considered practically immutable.
This has to do with the Proof-of-work mechanism, in fact, considering block with Alice's transaction, blocks after are defined as "confirmations" for that block. Any block with six confirmations (six blocks mined after) is considered quite irrevocable, because it requires a lot of computation and work to invalidate and re-create again the blocks. The longest chain represents the "truth" because it has the greatest Proof-of-work effort and cost.

2.8 EXISTING BLOCKCHAINS

Once defined the key technological features of Blockchain technology, now it's important to make a step forward towards applications of this technology to supply chain world, in particular to transparency.

First, Blockchain could be *Private* or *Public*; both are decentralized, immutable and based on consensus systems, the distinction is based on who is allowed to take part in the system. In Public Blockchains everyone can join the network and the most important is Bitcoin Blockchain (the one we have taken as reference to explain the key features), another important public Blockchain that is used in the case study is Ethereum Blockchain, while private blockchains require a permission or an invitation to join, set by an enterprise, an authority or a Consortium, and they work around cryptocurrencies created internally to the system. Once people have joined, they maintain blockchain in a decentralized way. In Private Blockchains people are expected to validate blocks even without incentives like in public blockchains.
Both protocols imply more transparency and decentralization than the current enterprise data systems. Anyway private blockchains are generally faster and require less costs to maintain consensus, but, due to the presence of a central authority, lack the total "trustlessness" critical of a public blockchain. So, managing supply chain transparency on public blockchains may be the best solution that today supply chain networks should adopt.

Bitcoin Blockchain was the original implementation of blockchain technology and the most famous and most widely used in the world. Anyway weaknesses and problems led to develop and study new blockchains that remedy possible shortcomings of the original one. This research has the principal aim of finding the best solution for facilitating other application beyond exchanges of currencies.
Let's proceed with a description of three alternative approaches being pursued in the industry:

- *Alternative Blockchains (Alt chains):* they are all blockchains (public and private) other than the most famous one, Bitcoin blockchain. Even if these ones are projected to overcome weaknesses and problems (explained in the next chapter), the key question may be how these blockchains can enjoy the benefits of the huge network effect of existing public blockchain.

  To be clear, no alternative blockchain has the value and the size of Bitcoin blockchain, but for some applications, other than exchanging "money", it's possible that they take important advantages.

  Alt chains include different kinds of blockchains; one group is private and permissioned with restrictions in terms of transparency, accessibility and transaction validation. Obviously the use of this kind of blockchain should be limited to cases in which the risk of complete openness and total accessibility is really perceived as vivid; this changes the level of trust required by the system, null in the case of public existing blockchains, as repeatedly stated, very high in the case of private blockchains with limited and single validators.
- *Colored Coins:* this approach uses Bitcoin Blockchain, in fact colored coins are very little, minima, unique portions of Bitcoin that have been defined as another asset, for example another currency, shares, or something different. The characteristic of Colored Coins is that they can take advantage of the network effect, of transactions and innovations of the Protocol; obviously transacting directly on Bitcoin blockchain is also limiting.
- *Sidechains:* Sidechains approach allows them to have the freedom to optimize particular features of their specific blockchains, maintaining the network effect of the main blockchain, through a two-way linkage between Alternative Blockchains and Bitcoin Blockchain.

Obviously every approach is right or wrong considering the surrounding environment and the context, considering the state of the art of the technology (deepen in the next chapter), everything is uncertain yet; anyway, for how many are the differences between the approaches above, they can enjoy the same structural advantages.
What researchers and entrepreneurs believe strongly is that blockchain solutions, network and peer-to-peer solutions are going to emerge more and more in different industries and they want to be close to these developments.

2.9 ETHEREUM AND SMART CONTRACTS

It's important to describe an important blockchain that has some differences with Bitcoin blockchain, but that is acquiring greater and greater importance with the progressive discovery and development of new applications for blockchain technology, beyond financial and payment system.
Ethereum was invented in 2015 when Vitalik Buterin published his white paper, with the main aim of developing a platform for smart contracts and decentralized applications. As in the case study described later, now it is particularly used for projects that deal more with transactions, rather than with payments and financial applications.
Smart contracts are one of the most curious and useful applications of Blockchain technology and are described by Buterin as "cryptographic boxes that contain value and only unlock it if certain conditions are met" (https://github.com/ethereum/wiki/wiki/White-Paper).
Decentralized applications are applications that run on different devices without relying on a central server, this means that these apps can't be attacked or hacked because, even if a node is attacked, the others are able to run the app independently.
Said simply, Ethereum Blockchain uses Ether, its cryptocurrency, generated in a totally different way than Bitcoin; an initial amount of Ether (quite 60 millions) was created and distributed among early contributors, developers or invested in projects on Ethereum and 5 Ether are given to miners every block added to the chain. The supply of Ether is not meant to decrease like Bitcoin but there is a limit of 18 millions per year.
In Ethereum, proof of work mechanism, called Ethash, rewards also the so-called uncle blocks (blocks that are successfully mined but not considered in the longest chain). This happens because a block is added on average every 16 seconds, and this facilitates a

faster transaction validation but also the creation of forks and the validation of blocks that can not be included in the chain.
Anyway in 2018 Ethereum is going to adopt a new consensus mechanism, Proof of stake, called Casper, that should work with consensus-by-bet, that expects nodes to pay a deposit and bet on the block they believe it will be validated to get back the deposit plus fees on the block.

A smart contract can be defined as a software protocol able to perform an action when certain conditions are satisfied; they work according to the logic "if this happens, then do that". Nick Szabo was the first, in 1997, to describe mechanism behind vending machines that work with a basic smart contract mechanism for which you receive an item only once the machine receives money.
Today and in the future, Blockchain-based smart contracts can add the same mechanism to many other daily tasks and applications; they are self-enforcing, set and written in programming code in order to be executed automatically by the system. Parties involved define the conditions under which their relationships have to be regulated, translate them in programming code and transfer contracts on blockchain to make them autonomous, distributed and permanent.
Between the advantages of smart contracts, there is the fact that they don't create controversies about interpretation of the terms and conditions. Furthermore they are self-enforcing, there isn't the need of going to the court to enforce the contract when when one of the parties violates the terms; the contract itself recognizes when clauses are not respected and is able to act in a way aimed to defend the damaged part. On the other side, smart contracts are public so readable and accessible by everyone, so although they can bring many advantages, they require a great sacrifice of privacy.
Let's make an example of a smart contract in everyday life; one airplane company decides to implement a new strategy to attract new users, for which their customers will be refunded 30% of the ticket price, if the plane lands with more than half an hour of delay.
The company is going to manage this mechanism with a smart contract set in the system; when a customer buys the ticket, 30% of the value will be put in an escrow account, if the delay is less than half an hour, the amount in the account will be unlocked and given to the airplane company, otherwise it will return back to the user. This may be

possible without the intervention of the company but automatically, using these self-enforcing contracts.
In the same way, as described later, the pilot project that tracks tuna fish from Indonesia to final consumers use smart contracts; everytime the product changes owner along the supply chain, a smart contract set by the system itself allows to enter automatically all the product-related information on blockchain, so that every actor can see them and be sure of their authenticity.

2.10 MAIN APPLICATIONS OF BLOCKCHAIN

After the discovery of blockchain technology, this has gained more and more credibility and many companies started to invest in this innovation. Obviously the immediate benefits were evident in the information technology field and in financial sector, where Blockchain was going to bring greater transparency and security to exchanges of value and information.
Before focusing in depth and exclusively on applications on supply chains, below there is a review of the most relevant and possible applications, not all, involving other industries and sectors:

- *Payments and Currencies:* after Bitcoin's success, other cryptocurrencies have been created and blockchain remains as their underlying technology layer. Decentralized issuance of digital currencies and the system of completely traceable payments remain the first and most famous applications of the technology. For example the service performed by Western Union of transferring remittance money from people living abroad to their relatives or friends in developing countries can be changed and be made by more easy and flexibile.
- *Exchanges and Stock Market:* beyond payments, Blockchain technology had a great impact on digital value exchange and on financial markets, especially in clearing and settlement processes. Exchanges regard both digital currencies and other digital assets on platforms created by companies (Bonds, gift cards, mobile minutes, etc). About stock markets, the idea of a decentralized stock market without power in the hands of governing power seems to be very interesting but for now remains only an utopia.

- *Digital Identity and Voting:* Blockchain technology could provide the right structure to invest in digital identity without sacrificing privacy and security. This application has an impact on governments and bureaucracy, in fact a decentralized identity system allows to see the information and reputation built by people in the network without relying on paperworks and documentation. This could also facilitate the process of voting and controlling the votes.
- *Smart Contracts and Smart Property*: in the field of legal applications, smart contracts and smart property are important use cases that may bring several benefits to other sectors and industries. As described above, a smart contract acts exactly like an automated contract; it allows to perform different actions (for example transmit information, make a purchase, etc.) when some special and set conditions are met. Consequently Smart Property could lead to the digital identities of many assets in the network, which, thanks to contracts, are able to "act" in the set way. Said simply, an example should be when a room door in a hotel becomes unlocked when the system recognizes that the user has paid.
- *Insurance and Ownership Rights Protection:* people can have direct control over their goods and manage, for example through smart contracts and smart property, accidents and claims in a decentralized, secure and transparent way. The idea is also to create a music and art industry in which artists have the chance to control directly their works and commercialize them at their conditions (i.e the singer Imogen Heap started using Blockchain to commercialize its songs).
- *Sharing Economy:* a presumption of Blockchain technology is to make sharing economy definitely a sharing economy, in which value produced is redistributed to the ones who generate this value. Now leaders in sharing economy that operate the platforms (Airbnb, Uber, Lyft, etc.) capture also the part of the value generated in the network, while blockchain technology could remove power and control from these intermediaries and make these network working in a real peer-to-peer architecture.
- *Internet of Things enabled by Blockchain:* today people have more and more connected devices, starting from thermostats, cars, domestic devices and appliances and etc. that work quite automatically, usually activating them with apps on devices or objects that give and collect information and data through

their connection with smartphones and other devices. Anyway the fact that today they work mainly in a centralized framework poses some problems that experts believe blockchain technology could solve; one problem is that it's fundamental that anyone using any connected device is able to verify independently that it performs its function without alterations or damages, and that it will continue to work suitably in the future, and this may happen easily thanks to transparency ensured by blockchain, in fact in the centralized model it's hard for all but the largest incumbents and companies to ensure people that they will be still operational with the same efficiency for the next years. Basically making IoT devices connected on a decentralized platform may facilitate transactions and coordination between them, that with different roles and functions create an "Internet of decentralized, autonomous things"; blockchain technology would perform some key functions related to the IoT, first it creates an immutable and distributed record of device identity, it can constitute a basis to create more smart contracts and finally it make possible the exchange of value also between devices. As evident in the case study at the end of the elaborate, Internet IoT enabled by blockchain allow physical products and entities to be perfectly interactive through technologies like tagging, coding, etc.

CHAPTER 3. BLOCKCHAIN AS INNOVATION AND DISRUPTION IN INFORMATION TECHNOLOGY FIELD

According to PwC, Blockchain is one of the eight most important recent technologies, that are going to have a great impact on worldwide economy, to consider and monitor today; these are Artificial Intelligence (AI), Augmented Reality (AR), Drones, Internet of Things (Iot), Robots, Virtual Reality (VR), 3D Printing and obviously Blockchain.

Researchers and experts, like Dan and Alex Tapscott in "Blockchain Revolution", that believe strongly in the potential of blockchain, think that it will have the same development of the Internet in the last decades; how Internet has created opportunities and new business models (for example Social Networks, sharing economy, etc.) to exchange value and information, so blockchain technology will ensure new opportunities of similar scale. Basically this new phase of Digital Age is bringing many possibilities, challenges, but also dangers and an uncertain future, since the change is happening immensely fast, and it is accelerating exponentially.

Blockchain technology lived an initial relatively calm existence in the first years (around 2010), then, as the technology has been developed, began to gain a wider recognition beyond groups of first-movers, since then advancements, applications, opportunities continue to increase immensely. It is presented as a radical innovation that is going to "disrupt" how value is exchanged today on the Internet. This determines an important step forward from the status quo, where transactions of value have always needed third parties, middlemen, intermediaries, consequently incurring in inefficiencies in terms of costs, delays, and risks.

An important factor for exploiting fully the potential of blockchain technology is that it, with network and ecosystems it creates, is able to enable "permissionless innovations": the "openness" and the peer-to-peer architecture of the network make possible that anyone can enter it, join the community, and build and develop products, services and applications available to other actors.

In the previous chapters, blockchain technology has been described considering its structural advantages such as durability, openness, immutability and transparency, especially in the field of supply chain, but obviously there are still many issues and perils that block the full mainstream adoption and application, that will be described in the next paragraphs.

3.1 TRENDS AND DRIVERS OF GROWTH

This technology emerged for the first time in 2009 and in its first years lived a relatively quiet existence; in following years its real potential started to become evident and it gained a greater recognition beyond groups of passionate followers, since there have been projects, ideas, developments that have more and more intrigued entrepreneurs and people.

Nowadays industries and companies are clearly starting to understand the potential of this technology and its applications, in fact early enterprise adoption, pilot projects, R&D investments and venture capital activity are all emerging trends that may suggest that blockchain technology is going toward an always greater mainstream enterprise adoption. In fact the magnitude of venture capitalists' investments in blockchain-related companies is accelerating year by year, and there are many companies and start-ups that develop important projects beyond standard applications in finance and payments. As described later, the blockchain industry has attracted many entrepreneurs and technology investors worldwide, that since 2012 have had invested heavily and increasingly in more and more specific and broad user-end solutions and applications, so much that Deloitte talks about a value-added of about 176 billion dollars by 2025.

The figure below illustrates the increasing rate of capital invested (in millions of dollars) from the first years of blockchain development.

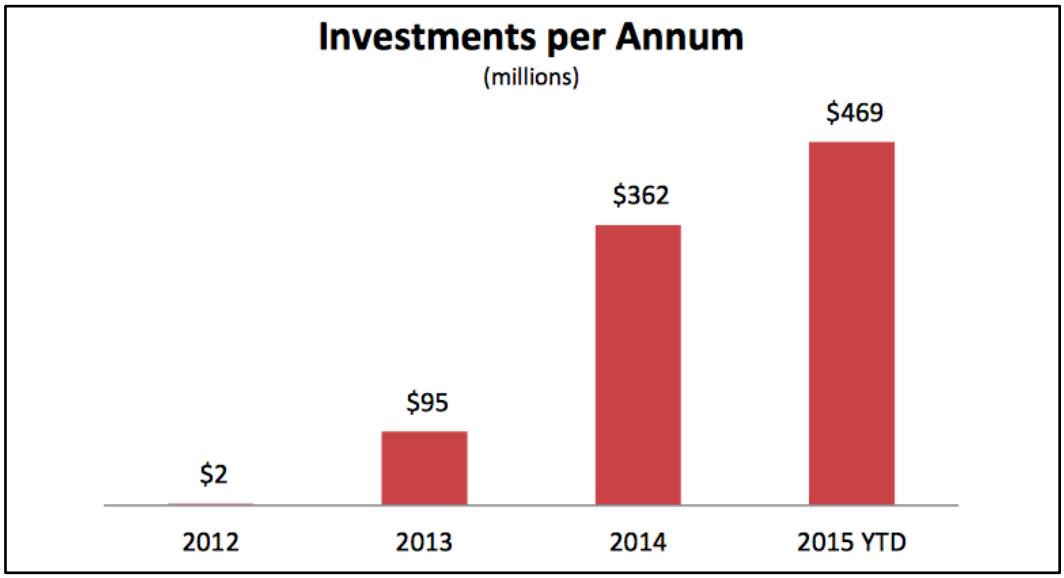

Figure 9 – Rate of capital invested in blockchain (Source: Welcome to the Interne of value, http://www.the-blockchain.com/docs/The%20Blockchain%20Report%20-%20Needham%20(Huge%20report).pdf)

Anyway the layer and infrastructure necessary to support and maintain a fruitful ecosystem and network of blockchain-based applications and products are being established following some growth drivers. As they grow, companies that adopt this technology are expected to flourish, gaining new economic efficiencies and promoting its mainstream application.

The first driver that determines the level of diffusion of blockchain technology is the *natural pursuit of efficiency and profit,* in fact companies and businesses that are striving to gain better profits, reducing costs or increasing revenues, believe in the potential of the technology and are starting to apply blockchain technology in particular to their supply chains, payment systems and to other business purposes.
Parallel to efficiency and profit, business people, especially considering in developing countries, start to notice *the Marginal cost advantage* that Blockchain technology may bring now and in the future. This represents a growth driver especially for developing part of the world and economies, because low marginal cost represents an affordable threshold that distinguishes countries, economies, businesses able or not to meet this threshold. Reaching a minimum threshold might mean bringing millions people more into e-commerce, home banking, digital world, etc.
Another important trend that is driving the adoption of the technology and it is determinant to establish the widespread adoption is the *Mobile phone access*; it is a critical and key element, fundamental to "democratize" the adoption of the technology. Considering that initially, when blockchain technology was defined by first academics and researchers, it was thought to enable people in developing countries to join the world economy, to join prosperity, to transact value without losing it, the mobile phone access would bring many important benefits in this direction. Nowadays, people in emerging economies are still quite outside "banking", transacting money directly or sending through services and intermediaries, they are outside e-commerce and digital world; with mobile phone access actions like money transfer, property management, legal contracts execution may become daily activities. In the case study, for instance, Indonesian fishermen use their existing (even if patchy) Internet connection and mobile phones to provide visibility and transparency from the very first steps of the supply chain.

Consequently, another important growth driver is *the adoption by Major Enterprises*, often leaders in their industrial sector, like for example Walmart, Maersk, IBM, etc. First, this is important to establish and spread the "network effect" to ensure an increasing widespread adoption; in fact while big businesses are launching projects, investing in the technology and developing products to exploit blockchain, its total potential value increases for all organizations in the marketplace. This adoption helps also to reduce public psychosis surrounding the phenomenon, particularly solidifying confidence in this technology in the mind of people that consider these companies relevant for their leadership, expertise and foresight. In particular Ethereum development has increased more and more R&D activity and projects based on it, and companies are exploring and adapting the technology according to their needs.

As described in the previous chapter, *Internet of Things enabled by Blockchain* is one of the most important and curious applications, that may have great impact on people's everyday life. The project around Internet of Things is to create a decentralized IoT system, founded on Blockchain infrastructure, that facilitates definitely transactions and coordination between interacting devices. As the number of connected devices increases, blockchain adoption throughout IoT ecosystem may rapidly increases as well, both upon businesses and common users.

In the same way *Smart Contracts* already exist and are developing at a rapid pace, the idea of building a robust and mature Smart Contracts platform may bring important benefits to supply chains, as described in the next chapter, in particular in terms of transparency across the network. The chance of automating business contracts with programming code may bring several benefits, especially in terms of cost and risk of error.

Considering data and information, people start to perceive a feeling of *"broken trust"* toward the web, in fact recent scandals of access to private data, to private Clouds, hacking photos and videos, have mined the opinion about cybersecurity and this has become a key issue for businesses and consumers. The fact that people feel unsafe and vulnerable of sharing their personal photos, private financial information, identity information makes them looking for better solutions that protect data and, Blockchain, with its promise of being completely encrypted and distributed, seems to be an efficient solution to this problem.

In particular this has changed the way payments are done and information is exchanged in the network; but other blockchain-based applications apply the same rule to other important areas such as for example digital identity, healthcare records, insurance, etc. For this reason the idea of "broken trust" is another important growth driver; users want to have control on their data and information and, as described in the previous chapter about the technological features, blockchain helps to put people in control of their data.

As explained later, *the Rich Ecosystem* that is being created, although it is deeply diversified and hard to be managed, probably will grow more and more and will enable collaboration and coordination in the development of products, that would lower the barriers to enter the industry. Said simply, the principal actors that should collaborate in order to provide a great leadership in managing this innovation are pioneers, venture capitalists, banks and financial services, developers, academics, governments and institutions, non-government organizations and users. As they are able to mature and develop, so they will be able to leverage the potential of the technology. Considering the current level of investments, this development seems to happen rapidly in the next years.

Finally, the development of *alternative Blockchains and Sidechains* may be the last further element that is driving toward a broader application of the technology; in fact, as explained in the previous chapter, sidechains in particular could help to explore new applications and functionalities, relying on the network effect of the biggest Bitcoin blockchain.

Beyond these specific trends, Deloitte in its Report "Tech Trends 2018" defines the latest common trend, that unites the companies and the actors that are launching important projects and business ideas based on blockchain, and this approach combines first, the focus of resources on concrete use cases and projects with a clear way towards the commercialization, second, a push towards standardization in "technology, processes and skill-sets" and, third, a lot of work aimed to integration and coordination of different blockchains within a unique value chain.

3.2 THREATS AND PERILS OF BLOCKCHAIN TECHNOLOGY

Like every time that a technological innovation breaks out, there is confusion about it and also in this case there is a vivid debate between who sees blockchain as a great opportunity for industries, or even for the whole world, and who thinks that, comparing, there are more problems and perils than strengths in it. Considering problems, two conceptions are admitted according the expert D.Tapscott, or they are reasons why blockchain is a bad idea or they are simply "implementation challenges to overcome"; for the aim of the thesis, the second conception is the most preferable, in fact problems are described in depth, but possible solutions are proposed as well.

The problems described below are problems identified by researchers and experts considering blockchain technology as phoenomeno per se, considering it at 360 degrees, and these are shared by all the projects that are approaching blockchain technology; once described the case study in the next chapter, other limits of the technology connected to the specific situation will be analysed.

The following points describe at best the critical issues that at the moment are limiting the total diffusion and adoption of technology:

- TECHNOLOGY NOT READY FOR PRIME TIME

  Maybe at the origins of all the technical issues, there is the question that no technical and process standards are set yet, in fact in these years the network has witnessed a proliferation of platforms and solutions in the whole marketplace, but it remains still impossible to see a unique solution emerging above others. It's important to state that nowadays the process of setting Standards is incomplete but ongoing, anyway actors in the network should ask themselves whether it would be worth waiting for standards set by competitors or having a proactive role in defining them.

  This first, very important paragraph analyzes the fact that the technology has some technical problems, some have been already explained in the previous chapter, that may mine the correct functioning of the infrastructure. Basically the first element to consider and to cite may seem trivial but it's fundamental; at the current state, the system is quite inaccessible to the average person. In fact many websites and interfaces are still user unfriendly, even if companies are working

to develop user friendly and simple-to-use interfaces, and there's not enough support for common people who are not used to this kind of experience. Just addresses, strings of characters that need interpretation, data related to mining activity appear tedious and uncomfortable to type, comparing to the typical researches made today on Google.

For this, first, in particular common people are required to act a behavioral change to align themselves in a system with greater trust, privacy and security and decentralization. Nowadays people rely strongly on intermediaries, like banks, companies, organizations, especially when they incur in problems like loss of credentials, errors, passwords forgottens, etc., but with blockchain technology more freedom as well as more responsibility are coming, and people should learn to have total control over their credentials and actions, forward-looking enough to keep these, for example, in safe or different places; in fact the rule that whoever loses his passwords and credentials, loses the money as well, represents one of the most scaring and braking threat for people approaching the network.

At the same time the system itself lacks the "transactional capacity" to take on board billions of people; like Internet at its very first months wasn't ready in terms of protection and inevitably cases of virus and malware bursted out, so Blockchain as an immature technology may cause similar capacity problems for the first unsophisticated users. Problems like systems failures or not predictable bugs may cause disappointment to the newcomers and users that may mine reputation about blockchain technology.

More specifically, one important reason for hesitation is the high latency of validating transactions; before, it's explained that transactions clearing and validation take around ten minutes and even if in some cases ten minutes is less than the time of functioning of many payment mechanisms, ten minutes may be a too long time in situations in which timing is a critical element, for example when people in the network need to interact and transact through Blockchain continuously and promptly, or when financial transactions are aimed to get assets tempestively, or when payments need to be certified and recognized within a certain timing.

Consequently the number of transactions per second, called Throughput, is maximum 7 transactions per second and it seems to be critical considering the

throughput of thousands of transactions per second in other circuits, like for example VISA. Experts and critics see increasing block size as a possible solution in order to collect more transactions, but this would worsen another important problem, the fact that the size of the blockchain would become too heavy to be managed by everyone.

Furthermore it's important to remember that every transaction can be considered completely validated after about six blocks more added on the chain, consequently to be completely sure that the transaction is happened in the right way people may take almost an hour of time, in any case shorter intervals than many current systems, but longer compared to seconds or few minutes in VISA circuit, for instance.

Considering technical dimension, the question of incentives remains a complicated question, as said before incentives in the form of fees on transactions and rewards are fundamental to maintain the network working. Charging fees is a critical but fundamental aspect; fees on transactions represent the marginal cost of validating every transaction and have a fundamental role in mining activity because, as explained before, the higher the fees on transactions, the higher the probability that this transaction will be included in the next block, and furthermore fees will represent the only reward once the limit of bitcoin supply will be reached. Critics sustain that increasing fees may become unaffordable for people, so block reward may be reduced and network security may decline, and finally this would represent a critical final consequence for the infrastructure.

As explained in the previous chapter, also the question of the forks (hard or soft) that threatens the Bitcoin system and consequently blockchain infrastructure is a controversial one. Anyway considering the aim of the thesis, it's enough to mention the problem.

As evident, the network is actively debating about potential weaknesses of Blockchain technology and infrastructure, starting from capacity until latency and throughput dimension, and about how to solve them, whether developing the actual blockchain providing better technical solutions or developing new blockchains. Anyway now it's too early to have a clear answer but critics, experts

and developers are strongly convinced that all the points before explained are not able to preclude an increasing broad adoption of the technology.

- UNSUSTAINABLE COST OF ENERGY

  The first important issue to cite is related to the scalability of the system; basically the larger the blockchain becomes, the greater are the requirements in terms of energy consumed, storage, bandwidth, etc. and, as already explained, this could bring to a sort of centralization in the system, since only few actors in the network would be able to run fully mining activity and transaction validation.

  As explained before, activities behind blockchain functioning waste an enormous amount of resources and electricity power. This is what makes the system completely safe and secure but the spent resources imply an enormous cost for people in the network. Just think that, according to D. Tapscott, the energy consumed by the network is comparable to 700 average american homes or to the energy consumed in the entire island of Cyprus, that is more than "4.409 billion kilowatt-hours". What is critical is that this will represent an incentive to centralization because it will be more and more difficult for a normal personal computer to manage and work with it, in fact today in the world there are only around 6000 servers able to work on it and to run the system; this is why developers, experts and actors in the network are working to find an immediate solution to the problem.

  This issue is something that concerns everyone, since citizens care about their planet; all this computing power, useful for many other actions of public utility like academic research, avanguard projects, big inventions, etc., is exclusively exploited to run the network and the infrastructure and requires an average expense of around 100 $ millions per year and a very large amount of carbon emissions to make it work. In fact the most advanced companies and start-ups are already relocating to places with cold climate where energy is cheaper and renewable, for example BitFury, an american company providing service on blockchain platform, has already two data centers located in Iceland and in Georgia and is going to acquire a Hong Kong based start-up specialized sustainable sources of energy, in order to reduce the ecological impact of the infrastructure.

Furthermore the higher the value of cryptocurrencies, the bigger the competition to mine and consequently the more the energy consumed for this activity; experts are trying to solve the problem making the proof-of-work efficient but for now the trend seems to be using more energy instead of less. Some other experts and developers think that the only way to reduce waste of energy is to change proof-of-work mechanism to reach consensus and to combine or replace it with other mechanisms or solutions, as cited in the previous chapter. The most explored alternative is founding consensus mechanism on proof-of-stake algorithm in order to secure the network maintaining decentralization, but anyway experimentation with proof-of-work algorithm is something to take seriously and with caution by developers and entrepreneurs, being a new area of computer science.

Another possible innovation to solve this issue may be so-called API, that allows to extract information and data on transactions from the blockchain without downloading it on the device. Other sources that work in the same way but that are more user friendly are web based block explorers (i.e. blockchain.info).

This cost of energy seems to be the cost for having no central power or control, and the most optimist critics believe that all this electricity and energy spent and consumed make sense because this happen for a specific and well defined purpose, a real service is given, that is providing security and privacy to transactions of value of any kind.

Basically experts believe strongly that "all forms of money have a relationship to energy"[2], just think that gold itself needs a great amount of energy to be created. So this great consumed energy and electricity should be compared to the cost of electricity spent by the current system, sustained by banks, intermediaries, financial institutions, to sustain their financial rules and infrastructure, like maintaining ATMs, branches, bunkers and safety vaults, etc. and it will be not completely clear which is worse.

- PUBLIC OPINION

  Another fundamental obstacle to mainstream adoption and diffusion of blockchain technology is the opinion people have about it but also about

[2] Stephen Pair of BitPay identified this analogy with gold in the current financial system.

cryptocurrencies; it's important to state once again that cryptocurrencies and blcockahin technology are two separate and distinct phoenomena, even interconnected, especially considering that from now ahead blockchain technology will have more and more applications beyond the financial sector.

Unfortunately in public opinion the two phoenomena are often confused and considered as the same thing, sometimes bad reputation and bad news around the world of cryptocurrencies may have influenced also the public opinion about blockchain technology.

Due to recent scandals, blockchain technology has been associated to untraceable and anonymous purchases on the "dark net"; experts are worried about it because this "numismatic delirium" risks to seriously overshadow the blockchain technology story. It's probably that blockchain technology struggles to reach mainstream adoption and diffusion just because it is too often associated to cryptocurrencies world in a negative way.

In fact, in the first years people viewed cryptocurrencies as a mean to drive illegal activities, like laundering money and dealing with illicit products; since the technology is decentralized and open, criminals try to exploit it. In 2013 Silk Road, a web marketplace for illicit drugs, had around 13 000 listings in Bitcoin; products were sent by mail with a manual to avoid controls of authorities, until FBI finally closed it. Obviously this episode made cryptocurrencies synonymous with crime. After 2013, there were some other scandals and frauds in the world of cryptocurrencies, in particular phenomena of website hacking. Another question is that recently Bitcoin and cryptocurrencies reached many people, not exclusively experts, passionate followers, etc. but also common people, that are approaching to this world, often without the necessary knowledge, than don't get the expected results and remain disappointed.

In reality experts say that blockchain has nothing particular that makes it more suitable for crime than other technologies; rather, with algorithms and cryptography and continuous monitoring of activities in the network, it should be able to foster law enforcement and to solve different crymes, like supply chain fraud and counterfeiting. Basically there's not a unique technology that has been proven completely unhackable, every new technology means new possibilities, for good and for evil, and crime will use the newest technology to do it,

technology doesn't have agency or "personal" inclination for good or evil, the fact that it may be used by crime would depend more on lack of regulation, governance, form of legalization, as explained before.

If people think in depth about the technology, they would understand that trivially every illegal transaction made on blockchain will be traceable permanently by everyone in the network, included legal authorities. The high level of certainty enabled by smart contracts that makes outcomes of contracts perfectly predictable, provides more security and more efficiency in performance but it lets no more room for "human" behaviour; then people feel confused about how to deal with the legal cause or, eventually, how to manage a legal recourse.

Paradoxically what makes people still hostile to blockchain technology is the lack of privacy they perceived from the system; in fact while blockchain was thought to ensure a certain level of privacy and anonymity, it generates also a degree of openness. Many feel uncomfortable and start asking what will happen to their privacy when the physical world will collect, communicate and analyze everyday life data and whether they may be able to maintain control over their privacy and their data or not.

Furthermore people may feel afraid of the disruption that blockchain technology may represent also in the labor market; generally technological innovations might disrupt labor market only temporarily, but after the first periods they create new jobs. This time the fear derives from the fact that blockchain platform is enabling radical automation, where computer code makes the work in place of humans in different fields, so the question posed remain if this automation will open new business, and consequently employment, opportunities or if it will cause unemployment in those jobs with routine tasks that require low skilled workforce.

- CONSENSUS ATTACK AND CENTRALIZATION

  This problem is an important threat to decentralization of the system; even if it is a less perceived problem by common people, it remains a concrete threat. This problem unites technical and social aspects and it deserves a complete paragraph because it endangers directly the fundamentals of the technology.

In fact, the consensus mechanism is threatened by miners with dishonest intentions to use their hashing power; this may happen when miners are able to have control and power over a significant amount of hashing power.

Said simply, the most famous possible attack is the so called 51% attack, where a large mining pool could control the majority of mining power (not inevitably 51%, but also less), causing, voluntarily, consequences like a fork, double spend transactions and deciding which transactions to be included in the blocks.

Obviously as the blockchain is spreading more and the investments to mine are increasing, there is the risk that an always smaller portion of big players will be able to enter or continue the mining activity. This may lead to the extreme consequence of centralization, paradoxical for a technology that promotes the decentralization as its first strength. Specifically one probable consequence is geographical centralization; for example considering the low price of electricity in China, a great amount of hashing power is in the hand of Chinese miners that could exploit this advantage to take control over the system, nullifying the attempts toward total decentralization.

Just to be clear, 51% is only a symbolic threshold that represents that this kind of attack is destined to succeed; then it's fundamental to say that consensus attacks may affect the future transactions.

- REGULATION

When companies and people started to adopt blockchain technology in their projects as immutable ledger of all the transactions, the problem of regulation became the biggest question mark around blockchain technology and inevitably this represents a big problem, in fact regulators and the "law" want to know how to qualify this kind of activity and what to do with it, perceiving that this would be a completely different kind of challenge and that this new technology can't fit in the already existing regulatory schemes.

In the past, pure peer-to-peer networks like Napster didn't succeed and were regulated, the question is whether blockchain network will be able to hold own against regulations and authorities or not. Legislators, regulators and institutions have already get it wrong, including, as a first attempt, blockchain technology in the legal field of intellectual property but it's not. The biggest risk is to not

understand completely the technology and the implications and to not have all the needed information, and consequently regulate it so heavily that the development of the technology may be harmed and investments diminished. There must will be a stable approach in the field of regulation and legislation, so that the network will be motivated to sustain the global development of technology.

Considering also the applications of blockchain, like smart contracts, smart property, digital identity, they would need a legal framework, different from the current one that is not able to solve the issues posed by blockchain infrastructure, so the question remains how and how much is possible to take old rules created for old technology and adapt them in the most rapid and competent way.

The resolution of regulatory and legal issues deals also with the question of standardization cited above; in fact to exploit the advantages of the technology, experts sustain that some standardization is necessary, to put some order about the functioning and the dynamics in the system. Consequently some places in the world, like some European countries and Latin America, are slowing down in using blockchain technology, because they are waiting for more standardization and regulation.

Also in this case, cryptocurrencies and blockchain technology are separate questions, even if interconnected, and some countries' governments decided to take different positions about cryptocurrencies and this had an impact on blockchain technology regulation as well.

At the moment governments around the world have not a completely clear and stable opinion over time; basically governments are limited in their scope of regulating, while blockchain platform is completely global in scope. Obviously governments don't have total power over blockchain technology, in fact they are not able to ban usage at all, but for now they are able to regulate if and how businesses and companies within the boundaries should use the technology.

Beyond governments, also the major financial institutions, like Central Banks, are not taking clear positions, some of them, like Bank of England, Bank of Canada and US Fed itself, are monitoring and studying in depth the development of cryptocurrencies, in fact in 2014 Bank of England stated that "digital currencies

do not currently pose a material risk to monetary or financial stability in the United Kingdom, given the small size of such schemes. This could conceivably change, but only if they were to grow significantly. The Bank continues to monitor digital currencies and the risks they pose to its mission" (https://www.bankofengland.co.uk/-/media/boe/files/digital-currencies/the-economics-of-digital-currencies). About Blockchain, Central Banks may be expected to oppose blockchain technology, while many of them react positively, understanding the importance of it also for their businesses and for the entire financial sector; in fact they see it as a new tool aimed to improve financial services, and secondly they are exhorted to answer some questions about their existence in relation to this new technology.

For example, Benjamin Lawsky, superintendent of financial services of the State of New York, understands the different and new value of this technology and faced the challenge proposing the "BitLicense" as first and immediate solution; but even if he acted with the best intentions, it appeared clearly that this was not the best solution, in fact putting a costing license caused that companies moved away from New York, leaving there only mature and capitalized companies. Finally critics asked whether BitLicense should be a right solution to manage the innovations or not, the general idea was that it used old paradigms to new problems.

So as described later, more than regulating, the aim is finding a governance framework or model able to manage these resources in order to improve viability and to exploit the potential; creating a right governance model may mean setting standards, adopting right policies, researching and developing knowledge about the technology, monitoring the functioning and investing in building a globally spread infrastructure. It must be clear that it's more a question of governance rather than regulation; in this phase it's fundamental that governments for first should use caution and collaboration, acting with common interests.

3.3 THE BLOCKCHAIN ECOSYSTEM

Starting from the regulation problem cited above, over the years, from the most remote ages, organizations and industries were hierarchical by design because this was the

predominant paradigm, but with the digital revolution this model is not anymore suitable for new challenges posed, so it's necessary a radical change from the traditional model of governance, and, even if blockchain technology may ensure by nature several possibilities for everyone, the humans are the only ones able to determine the final outcome.

Innovations like blockchain technology embrace more concepts like openness, coordination and collaboration; so people in the network are looking for an efficient model of governance, or more precisely of leadership, rather than regulation. For such global and complex kind of innovation, governance provided only by governments alone is not enough, the same goes for the private sector.

In fact experts are convinced that, to make blockchain maintain its long-term purpose and continue its evolution, all the stakeholders in the network, governments, individuals, private businesses, should lead and govern the innovation management and provide good leadership, starting from education towards this new model of governance. It's more a debate about the opportunities to be catched by leaders in order to manage efficiently this global resource.

It's important to see who these stakeholders are and which is their role in the network. Obviously this new infrastructure attracted different stakeholders with different backgrounds and goals, like investors, governments, individuals and users, industry players and so on; with the advent of the Internet, stakeholders of different size became able to use the new means created by the system to collaborate.

Let's see who these main actors are:

- BLOCKCHAIN INDUSTRY PIONEERS

  There are many powerful companies that approached almost for first to the technology and are continuing to capture the value of it in order to exploit its potential and this constitutes an important driver of growth, as said above. These companies that are building their blockchain-based success in different industries, from food to fashion, are trying to catch all the opportunities; probably the initial push was that, with the digital revolution, the risk was of being the ones left behind, and no one would have loved it. Between the big companies that are launching projects with blockchain technology, there are IBM

that launched the IBM Blockchain, a platform to help other businesses implement the technology, Samsung, Walmart, etc.

These companies believe that blockchain is already well-regulated by mathematics and informatics, anyway, as the industry grows, entrepreneurs and businesses are building a constructive dialogue with institutions, governments, etc. The risk is that large incumbent companies may lobby in order to have rules created for them get applied also to small start-ups or newcomers.

In fact powerful incumbents should continue to study how the technology meet customers' needs, how to develop other applications and challenges, and this is possible only collaborating with others in the ecosystem through partnerships or acquisitions, in particular start-ups, consortia, etc., not hindering them.

- VENTURE CAPITALISTS

  Over the past years venture capital investments in blockchain-related industries are largely increasing and accelerating, starting from 2012, in fact from two million dollars in 2012 they became 500 million dollars in 2015. This first wave of investments is flowed mainly to companies involved in managing wallets, payments and transactions; nowadays the second wave of investments is directed to companies that focused on broader applications, and finally people in the network expect a third and last wave of investments, aimed to invest in the most rich and determinate end-user applications.

  Many financial investors and companies, like Goldman Sachs, JP Morgan, Barclays, VISA, Deloitte, took part in large investments in start-ups or projects supporting the technology, for example Quorum by JPMorgan is an open-source platform created to implement smart contracts and enterprise-ready solutions for financial sector.

- BANKS and FINANCIAL SERVICES

  Actors in the financial sector lived a long dilemma, in fact in the first years institutions felt hostile towards blockchain technology but now are changing opinion. The most famous banks of the world have already joined the R&D projects and taken part in the leadership question.

- DEVELOPERS and CONSORTIA

  Developers have the main role of working on technical issues and on making sure that the technology sustains all the other activities based on blockchain. Anyway they are concerned also with the leadership. Blockchain Consortia, like Enterprise Ethereum Alliance, Hyperledger Project, R3 and B3i, are developing a serie of blockchain-based firm solutions.

- ACADEMICS and RESEARCHERS

  Universities and academic institutions are creating labs and specific centers to study the technology, understand its features and cooperate with other actors. The approach of these actors is different because universities are places in which it's possible to conduct research activities, assessment sessions, stating technical problems without any special interest or biases. The most prestigious universities in the world, Stanford, Princeton, New York University, are promoting academic courses, conferences and workshops about blockchain.

- GOVERNMENTS, STATES and REGULATORS

  As said before, governments have a different approach, some adopt the "laissez-faire" approach, others deal with regulations and rules and others show their clear hostility. For example, Benjamin Lawsky, superintendent of financial services for the state of New York, believes that strong regulation is necessary to ensure industry growth. They should change their traditional role of top-down enforcers and become active players in a bottom-up governance and diversified network.

  Regarding cryptocurrencies, countries are taking clear positions and, for instance, some authoritarian states, like Bolivia, Bangladesh, Ecuador, banned the use of Bitcoin. Regarding blockchain technology, the figure below shows the impact of blockchain technology at a global level, measured in the most important geographical areas according to relevance, timeliness and readiness.

  It's evident that blockchain technology has great relevance in all the areas of the world, except central Europe; the most ready areas seem to be Europe, Africa and Middle East.

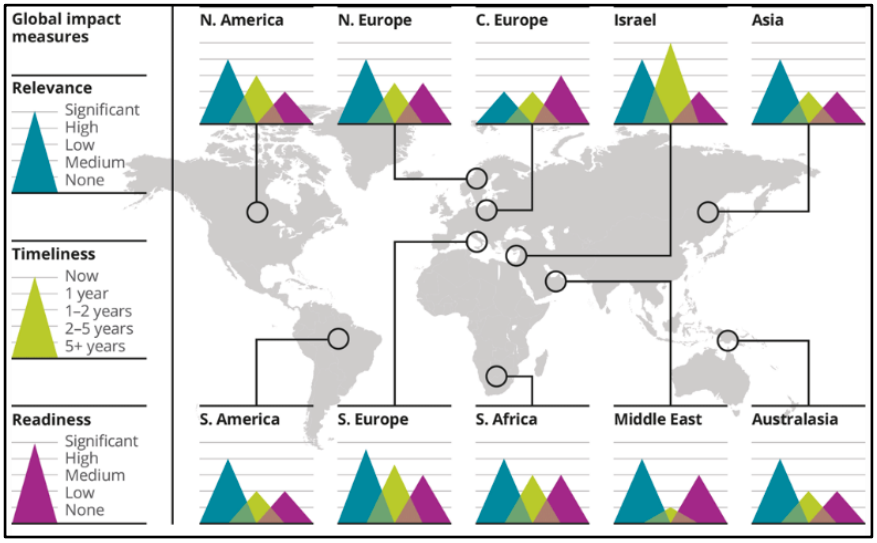

Figure 10 – Global impact measures of blockchain technology (Source: Tech Trends 2018, Deloitte Insights)

- NON-GOVERNMENT ORGANIZATIONS

  Said simply, since blockchain technology is aimed to increase prosperity and inclusion also for developing economies, there are also many NGOs and civil society institutions that are approaching to the technology. Their main role is "social", to spread it and to teach among communities the consequences and the advantages. It's important to specify that only in recent years NGOs and Academics have gained the chance of playing a role in the global effort ecosystem.

- USERS and PEOPLE

  That is mainly you and others like you, "common" people caring about key questions like identity, product traceability, privacy, asset management, etc. They feel a little bit confused about basic concepts regarding blockchain technology and its applications, but they are also the actors that may have the greatest impact on technology spreading and consequently on leadership.

- WOMEN in BLOCKCHAIN

  Blockchain industry is driven by many men, however high-profile women are leading companies and ambitious projects. For example Primavera De Filippi, faculty associate at Harvard and researcher at the National Center of Scientific Research in Paris, believes strongly in blockchain and she is one of the most

influencer organizer that works to build a dialogue with the ecosystem. She, with other women operating in the field, organized workshops at Harvard, MIT, Stanford, but also in London, Hong Kong and Sidney, where they put together people with different opinions, backgrounds and beliefs.

Perianne Boring, a journalist and TV reporter, founded the Chamber of Digital Commerce in Washington, where she tries to constitute a structured blockchain governance ecosystem with daily life activities, exploiting her background in journalism.

In the field of supply chain transparency, many women are doing fantastic works in their organizations and companies to solve the problem of lack of transparency, first Jessi Baker, CEO at Provenance, the company that developed the pilot project involving Indonesian fishing industry described in the next chapter.

Finally, it's evident that the actors in the field are numerous and really diversified, on the other side the disruptions are changing so rapidly, with a too different pace from the capacity of individuals and institutions to comprehend them, to adapt and to manage. This rhythm of innovation would require an acceleration in the human transformation as well, until all the parties listed above reach a common understanding of the situation in order to manage it at their best.

For example, the solution proposed by Dan and Alex Tapscott is that, beyond the blockchain ecosystem itself, actors should combine and create the so-called Governance Networks, and every network plays an important role in terms of leadership and governance of the technology; they think there should be ten different types of network, for example Knowledge network, Advocacy network, Watchdog network, Networked institutions and so on. Nowadays there are already existing examples of these, for instance The Blockchain Alliance is the first true Advocacy network created by a partnership between NGOs, law and private sector institutions.

CHAPTER 4. A CASE STUDY – TRACKING TUNA ON BLOCKCHAIN

The main goal of this case study is to bring a proof of how blockchain technology could constitute the basis for an open system of traceability aimed to improve transparency in the supply chain and in the network, ensuring at the same time compliance to international standards regarding food industry.

First, it's fundamental to specify why this specific project has been chosen; at this phase of the elaborate, it's important to find a project that shows this at best.

Anyway at this moment, in which blockchain technology as innovation is still far from mainstream diffusion and adoption and mainly applied to financial sector, projects that apply blockchain to supply chains of consumer products are still few and rare, and surely the Provenance's one is one of the most complete and detailed.

In fact the project of Provenance covers the whole tuna fish supply chain from phase zero to the end, not leaving out any actor of the network, but rather descibes in detail for instance the first passage of fishermen providing tuna fish in the form of raw material. This has been relevant in the choice of the case study considering that other similar projects, with the same final mission, proposed also by major enterprises with great experience, lack data and information, relevant to illustrate the functioning of blockchain technology.

The choice has fallen on the tuna tracking project considering also the mission and the engagement of the Company itself, that seems to be deeply committed to enhance transparency of consumer products through blockchain, they acquired expertise and knowledge of International Standards and "green" practices and they developed a technology mainly based on blockchain technology. Along the report that describes the project, it seems that Provenance illustrates every step in great detail, particularly regarding the research and analysis phase, the method and the intentions, enriching with clear and immediate images; although some information were not disclosed also when privately requested, it is possible to assume them with quite high reliability.

4.1 INTRODUCTION ABOUT PROVENANCE

The case study describes a six-months long prototype project, still in development, of 2016 conducted by the company Provenance, a London-based start up managed and

founded in 2013 by the entrepreneur Jessi Baker together with some colleagues, on the fishing industry of Indonesia; they describe their company as "a platform that empowers brands to take steps forward toward greater transparency by tracing the origins and histories of products. With our technology, you can easily gather and verify stories, keep them connected to physical things and embed them anywhere online" *(https://www.provenance.org/about#mission).*

Behind the business mission, Provenance has also a strong and vivid social purpose that drives application of their technology to supply chains around the world; in fact the alignment between business operations and environmental and social standards is a priority, aimed to maintain and improve ethical labour practices, environmental preservation practices, eliminate fraud and bad practices along the supply chains.

Basically Provenance addresses the vivid problem of today globalized supply chains: many lack information around products they buy and, as said before, this is paradoxical in a world that seems to be more and more connected and well-informed.

In the first chapter it is stated that actors, along the whole supply chain, from suppliers to importers and customers, need better access to information about products, and Provenance wants to show how to solve the problem of lack of data, without relying on centralized information systems but instead on a decentralized network.

Provenance uses a completely innovative technological paradigm to pursue its mission; as described in their White Paper, they combine blockchain technology with mobile, Internet of Things, smart tagging, new technologies of identification, etc. to track goods from first suppliers through factories and points of sales until the final customer. Before developing, the company conducted a deep research to understand the problems, assess the possibilities and then elaborate the final project, considering both technological, business and sustainability aspects.

Anyway, the idea of Provenance is to found its work on the already existing efforts and commitments of companies, considering also the existing partnerships like This Fish, USAIDOCEANS and Fair Trade USA. Rather than working on completely new technologies and data collection systems, they want to use the already made efforts and spent resources as groundwork to build their infrastructure, that may become the first and base layer of truth about products.

The description of the case study is taken directly from the Provenance website (www.provenance.org); to describe it in the clearest way, both the specific report about

the tuna project and the White Paper that explains the technology used by Provenance in all its projects have been used.
Just to be clear, some information, like the details of the functioning of the smart contracts, the specific blockchain used and the costs of the project are not present in the website, they have been asked directly to the company by mail, but they didn't answer; anyway some of them are deductible with quite high reliability and certainty.

The main objective of Provenance in developing this pilot project is to improve history and operations transparency. In concrete this is possible with:

- Better and clear connection with downstream and upstream actors of the supply chains
- Accessible information about impact on local communities and commitment to good and ethical practices, bringing elements of product's story to be part of consumers' selection process.
- Definition of open traceability standards for products and interoperability of data.

4.2 INDONESIAN FISHING INDUSTRY TODAY

To implement this project, Provenance focused on the SE Fishing Industry of Indonesia, which seemed to be a complex globalized industry and consequently a perfect playing field to apply blockchain infrastructure to improve traceability.
In particular Provenance has developed a technology able to track tuna fish captured in Maluku, Indonesia, and it has worked closely together with a community of fishermen there.
Indonesia is one of the largest country producer of tuna in the world and tuna is the one of the most exported products; people, more than 60 millions, live organized in coastal communities and fishing industry is the greatest source of employment and trade. Companies are often family-owned, involving different generations of fishermen.
But the industry is threatened by many weaknesses due to lack of transparency in the network, in particular bad practices like human rights violation, fraud, illegal, unreported and unregulated (IUU) catches of tuna, overfishing, bad data reporting are issues that weaken Indonesian fishing industry; just to say, for instance in the north of

indonesia, tuna fishing is threatened by Philippine tuna fishermen, that fish with purse seiners not recorded on the system.

In the past, tuna fishes were captured using traditional techniques, like pole-and-line and handline fishing, that required high-skilled workers and that created a high quality raw material. These techniques have always created the main source of jobs in the community and had a very little impact on the habitat, in fact they have been defined as "green" by NGOs and considered as a fine component of companies' sourcing commitments.

Said simply, pole-and-line fishing is the practice in which every fisher uses a pole-and-line to catch only one fish at a time. Handline fishing is the technique in which every fisher holds a single fishing line in their hands. Fishing with purse seiners means that fishers use large vessels or boats with large fishing nets hanged in the water.

In the last decade, globalization and industrialization have changed fishing industry and have increased usage of larger and automated vessels and boats with large nets, able to capture more tuna but probably of low-quality and employing less fishermen. Furthermore the precarious transportation and communication infrastructure of this developing country makes it difficult for importers to differentiate high-quality tuna from fish caught with other techniques or other fisheries.

Final exporters, such as major American, British and European retailers, probably ignore that tuna producers often work under slave conditions, with no pay or under threat of violence.

Between all the fishing practices, pole-and-line and handline fishing are seen as more sustainable from a social and environmental point of view, anyway they are not rewarded for this, and analyzing the trend since 2012, pole-and-line fisheries have been in a state of decline and many disappeared (Gillet, 2015); just think that small-scale pole-and-line and handline fishermen are facing many problems today, first, the unsustainable competition with larger vessels, often not registered and not regulated.

Obviously organizations and NGOs, like Marine Fisheries Advisory Committee (MAFAC), Indian Ocean Tuna Convention (IOTC) and even the FAO and Greenpeace, are the first who are worrying about the sustainability of the industry and the fate of the community.

The trigger that pushed definitely Provenance to develop a possible solution is the call from actors like final customers, governments, NGOs and importers for more information and a better transparency.

4.3 THE FIRST PHASE: RESEARCH and ANALYSIS

To develop its project, Provenance focused on two different supply chains:

- Yellowfin tuna loins (some of which were Fair Trade certified) from fishermen in Asilulu to Harta Samudra in Ambon.
- Skipjack tuna species caught by The Teluk Mas pole and line wooden boats in Ambon for production at a local cannery.

Provenance team met stakeholders and heads of eight fishing organisations, for instance fishermen, engineers, General Managers and Quality Assurance (QA) officers, all members of AP2HI, the Indonesian Association of Pole and Line and Handline Fisheries.
Companies involved are PT Samudra Mandiri Sentosa, PT Sinar Pure Foods, PT Chen Woo, PT Nutrindo Fresfood International, PT Intimas Surya, PT Hatindo Makmur, PT Harta Samudra and PT Aneka Sumber Tata Bahari.
These eight companies are all pursuing the production of sustainable and ethical seafood; they are deeply included in the local community, also as employers. They work actively to have the lower impact on environment, and to pursue ways to limit waste and promote sustainable fishing practices, also working towards international certifications, for instance Fair Trade and Marine Stewardship Council.
Through collection and analysis of data, Provenance mapped the supply chains and analysed current data collection practices, level of vertical integration, key stakeholders and technology capabilities.

As illustrated in the figure below, all the companies involved during this phase use systems like, clockwise from top left, digital labelling, Excel files and reporting, can printing, ipad data collection, but also pen and paper accounting of materials going in and out the facilities.

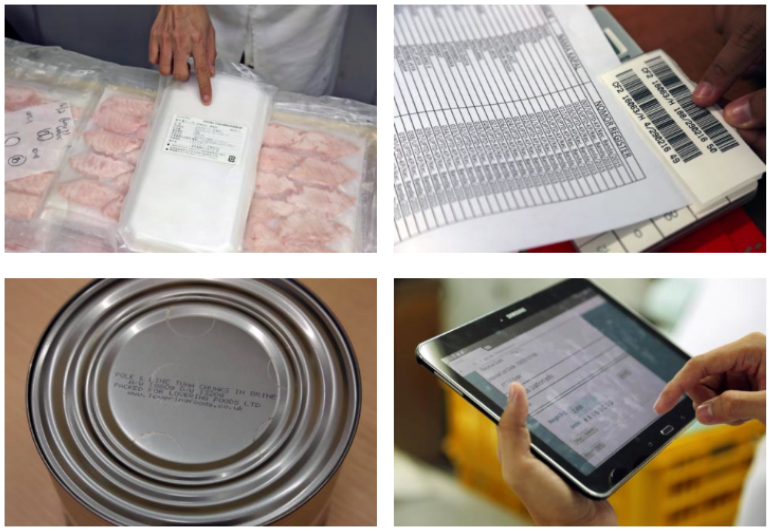

Figure 11 – Current methods of data reporting by Indonesia companies (Source: https://www.provenance.org/tracking-tuna-on-the-blockchain)

For instance, only PT Harta Samudra used already a form of digital accounting and traceability for fish using the ThisFish Tally-O initiative, developed by Ecotrust Canada; they were able to obtain Fair Trade certification for fish thanks to plastic tags put on tuna loins to identify who the fisherman is. Anyway, existing initiatives of this kind (for example ThisFish, Trace Register, etc.) are all attempts to digitise data but they don't have yet the ideal approach for making data completely interoperable and distributed, without single points of failure.

During the analysis phase, Provenance found that fishermen, suppliers and workers had a mobile phone and a 3G or wifi connection, it was patchy but completely accessible by the majority of towns.

Specifically in the report on Provenance's website that describes the project, Provenance team never specifies clearly which Blockchain they consider for this project. Anyway, since they specify that prefer public blockchains rather than private blockchains, the hypothesis is that they use Ethereum blockchain, the most popular and suitable for implementation of smart contracts and Internet of things enabled by Blockchain.

4.4 THE SECOND PHASE: REGISTRATION AND DATA COLLECTION

Before describing in detail every passage of the project, it's important to clarify two key points.

First, the actors in the network that took part in the project are:

- Registrars, that provide identities and credentials to actors.
- Certifiers, that provide different kinds of certifications to actors.
- Standard organizations and Institutions, that assess the standards schemes (e.g. Fair Trade, etc.).
- Producers, suppliers, fishermen, shippers, manufacturers, retailers, etc.
- Consumers.

Then, it's important to state that the supply chain is simplified compared to reality, in fact it considers:

- the first step of fisherman catching tuna fish.
- the passage from the fisherman to the first suppliers.
- the phase of transformation of tuna in the factory.
- the final phase of the consumer experience.

These are the type-situations described, used to explain how blockchain change the way these specific transactions work; obviously there may be many other transformations and passages along the chain, but the functioning is similar to the ones described below.

In this phase, Provenance worked with local fishermen, who catches the tuna, and the suppliers of two supply chains cited above to see how it's possible to register the initial transaction of tuna from the fisherman to the first supplier; all this first phase of the project is schematized in the figures 12 and 13 below.

Each actor joins the network of blockchain through a specific user interface, in the project the interface is the Provenance application interface itself, illustrated in the figures below, or linking Provenance application with other existing interfaces or systems used to track. The application is set considering specificity of products. It is perfectly accessible to standard organizations, institutions, certifiers, fishermen, producers and consumers that are able to access data about products.

The first step is the registration: in fact on Provenance, everyone may request the registration of his digital identity, linked to real-world identity, fundamental to form trusting relationships with others. The registration is possible through a registrar service, which is a service that gives credentials and unique identities to the parts.
Profiles can be public or private, have few or many information, depending on the role and the function.
Identities registered are then certified and inspected by Standards organizations or certifiers, which have the main role of assessing that identities, facilities, processes, etc. are completely adequate.
Considering the White Paper of technology used in Provenance, upon the registration phase, a pair of public and private keys are generated for each actor accessing. Basically public key identifies the actor in the network, private key is fundamental to authenticate the actor when interacts with others. This allows the products to be constantly digitally signed by all the actors, passing through all the chain.

In particular, for example, the fisherman's identity is registered on the system (in the example Lutfi), including data like name or place of fishing; their environmental and social conditions are verified by a trusted local NGO, that Provenance itself uses to verify that it has an audit system compliant to external standards. Some of the attributes tested are Fair Trade USA, Pole and Line Foundation Association Membership and GPS. Certified attributes are perfectly consultable on fisherman's profile, digitally signed by certifiers or standard organizations.
Then, once the fisherman captured a tuna catch, he has to send a simple SMS message to register the products on blockchain and starts the process of registration of the physical products as digital items on blockchain.
The SMS message is probably linked to an automatic smart contract; once the SMS is received, profile of the product (in the raw material configuration) is created officially and updated in the system. In this way the physical item obtains a digital identity.

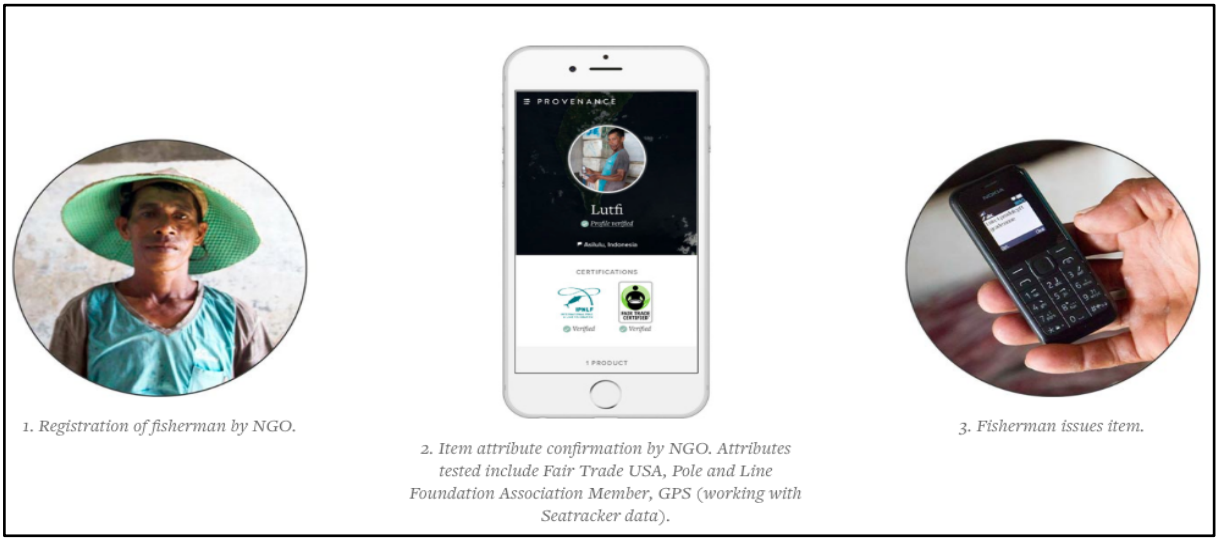

Figure 12 - Phase of registration of fishermen (Source: https://www.provenance.org/tracking-tuna-on-the-blockchain)

Every item is identified by a permanent and unique ID (for example, as shown in the figure 13, 75374); the asset can be now transferred from the fisherman to the first supplier, both physically but also digitally on blockchain.

Then, using a blockchain explorer like Etherscan, anyone is able to track and check the state of the digital asset, that represents the catch; it will ensure all the history, including details, of the item from the very first moments.

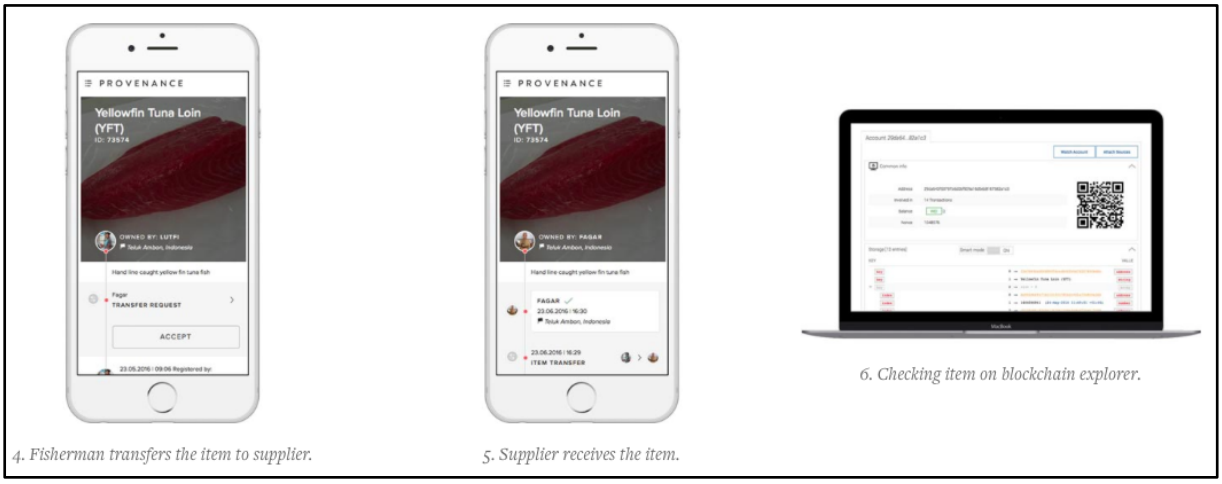

Figure 13 - Transaction between fisherman and first supplier (Source: https://www.provenance.org/tracking-tuna-on-the-blockchain)

But how does this kind of transactions work in concrete?
What is central and fundamental in this project is the application of smart contracts set in the system and created for the products, so that only the parties with the adequate keys have access to that contract.
First, the fish is "owned" by the fisherman Lutfi, only he is able to enter information in the tuna's profile. Then he sells tuna fish to the supplier, both parties sign the digital contract with their private keys to autenthicate the transaction. Once signed by both parties, the transaction is authenticated and permanently stored on Ethereum blockchain paired with a timestamp (data and time of transaction), accessible to everyone.
The system updates the permissions, so that only the current owner is able to update information and data about the product and to create new entries, using his private key to authenticate himself.
Data and information about the product, like time stamping data, location data and ownership data, are automatically updated when the transaction happens; while other data, like product specific data or environmental impact data, are added by the owner himself.
Obviously even if now the supplier owns the items, the fisherman will remain always in the system as the previous (and first) owner of tuna.

4.5 THE THIRD PHASE: PRODUCT TRANSFORMATION AND CONNECTION TO OTHER SYSTEMS

In the third phase of the project, tuna is transferred from the supplier to the factory, in which it is transformed into new products, like tuna cans, fresh tuna, etc. and consequently the digital asset on blockchain should be "transformed" as well, updating it. This is the type-situation taken to explain the project; anyway every transfer of the product from one actor to another one is expected to be registered on the blockchain ledger in the same way, as described above.

The most trivial example is that tuna fish enters the factory as raw material, but will leave it divided in different cans, each of which needs inevitably to be traced separately, as evident in the figure 14 below.

At this moment, Provenance uses always a digital process contract with open source and publicly determined and specific conditions.
An example of a process contract may be the one which uses mass balancing, that it is a method used to take into account the amounts of ingredients used in every transformation. For instance, it's been calculated that, to produce a can of Fair Trade skipjack tuna, 200 g of skipjack tuna and 10 ml of olive oil are needed; these details are included in the process contract, so that actors are able to understand how the transformation happened and how the identifiers are changed. In this way blockchain acts as in the real world: an output can be created if and only if required input is used.
According to the process contract, the registration of 10 tuna cans requires as starting input 2000 g of tuna and 100 ml of olive oil.
In this case the transaction works as said in previous paragraph, with authentication by parties involved; anyway this kind of transaction, that implies a physical transformation of the product, is based on a smart contract that allows supply chain actors and partners to check if "input" items correspond to the "output" items, in this way everything is traced and no items risk to be thrown, lost, modified, etc.
Then, after the transformation, every new item transformed (for example every tuna can) acquires a new identifier in the system, the previous one is physically destroyed or thrown, but information remains intangible on the blockchain. Even if the product changes "shape", it has a unique digital profile containing all useful information, integrated during different life cycle phases.

As said before, today mainly paper records or tags are used to track products along the chain, but with the digitalization of the chain, it's important to use technologies that allow the interaction between physical and digital world. Said simply, the technologies that are used are QR code, which is a printed code easily readable by a phone camera, RFID or NFC tag, that are small tags able to store and send Electronic Product Codes, attached to goods but not necessarily in the line of sight of the reader, and other similar hardware technologies.

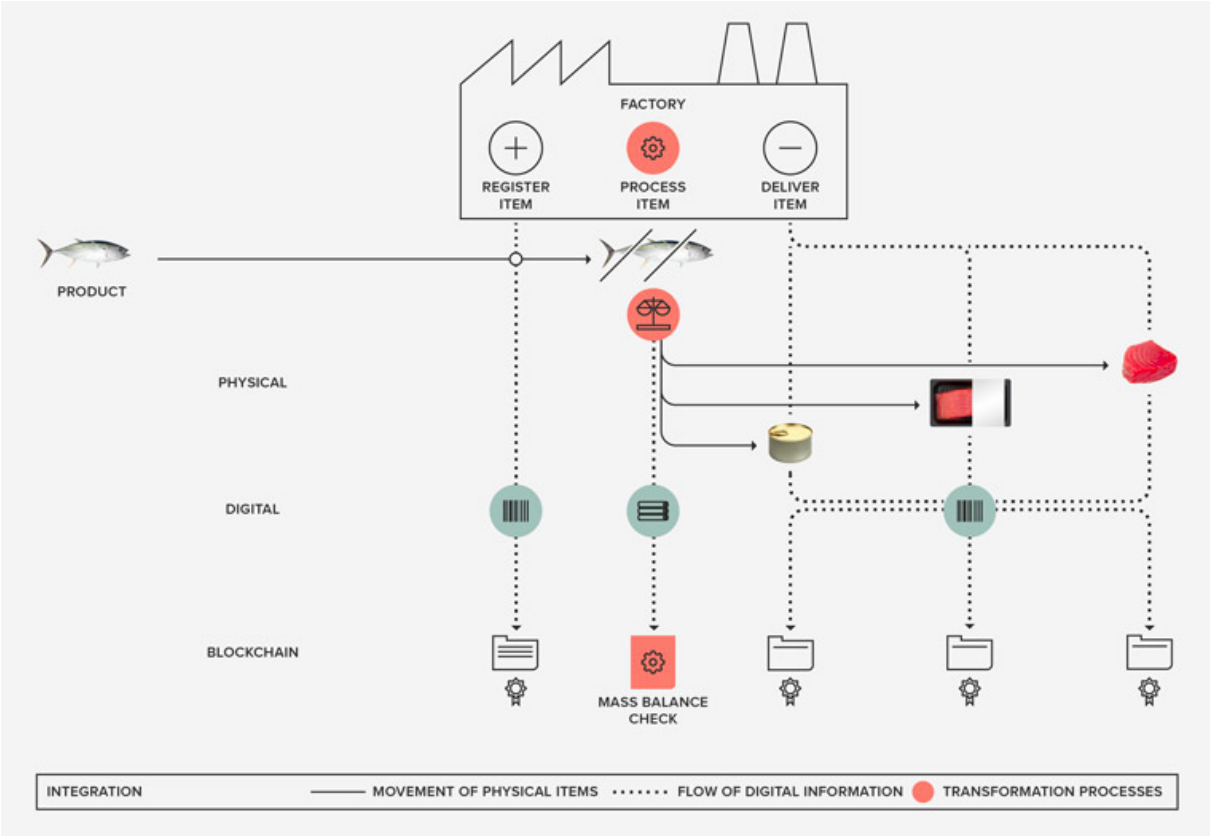

Figure 14 - Phase of physical transformation of tuna (Source: https://www.provenance.org/tracking-tuna-on-the-blockchain)

In the same way, every physical transformation or movement of the product, like packaging or shipping, is stored on the blockchain as a single transaction, while still being recorded by the usual and current informative systems of the separate actors. ERP and data management softwares are still in use, but now blockchain represents a base audit layer sitting on top of them, which makes decentralised data sharing possible between multiple actors.

Also in this phase there are audit inspections or certifications made by organizations and certifiers, aimed to assess and provide requirements like certification of the production capacity for that product, description of the products with some attributes (fair labor, fair trade, etc.), production accounting, etc., consequently these requirements are perfectly consultable on blockchain.

4.6 THE FOURTH PHASE: THE CONSUMER EXPERIENCE

The fourth phase corresponds to the last phase of the supply chain, when the product reaches the final customer.

To develop this phase and to assess the possibility of integrating Provenance into retail environments, Provenance conducted a workshop and in-store prototyping session with local Brighton supermarket hiSbe (how it should be) Food CIC.

Just to be clear, hiSbe Food CIC is a community interest company founded by two sisters, Amy and Ruth Anslow, where the profits are for community benefit rather than private advantage and the choice of the products is based on ethical, qualitative and green criteria. Provenance team met the founders at the Digital Catapult Center in Brighton.

This workshop gave Provenance important and different insights on consumers' behaviour, giving relevant ideas about how the technology could be applied in the scenario of supermarket.

The strategy, developed in the supermarket, but appliable to other retail environments like restaurants and fishmongers, is to use NFC tags and in-store tablets, to enable stories and journeys.

Below, represented also in the figure 15, some examples of application of Provenance technology in final point of sales:

- NFC tag upon tuna cans or packaged tuna on supermarket shelves.
- NFC tag upon menu, where tuna appears as an ingredient of dishes.
- Smart menu designed for Premium brands and products.

Figure 15 - Internet of things technologies enabled by blockchain in Points of sales (Source: https://www.provenance.org/tracking-tuna-on-the-blockchain)

In fact, customers via tablets are able to take a photo of the product and view the whole story of it, from the first fishermen, including shippers, exporters, shippers, etc. This definitely opens an era in which people would be perfectly conscious and aware of the proven origins of the product.

In the figure 16 it's represented the whole supply chain, every step recorded and consultable on blockchain; what is interesting is the continous and permanent parallelism between physical and digital world, everything happens in the physical world corresponds to digital representation on blockchain ledger.

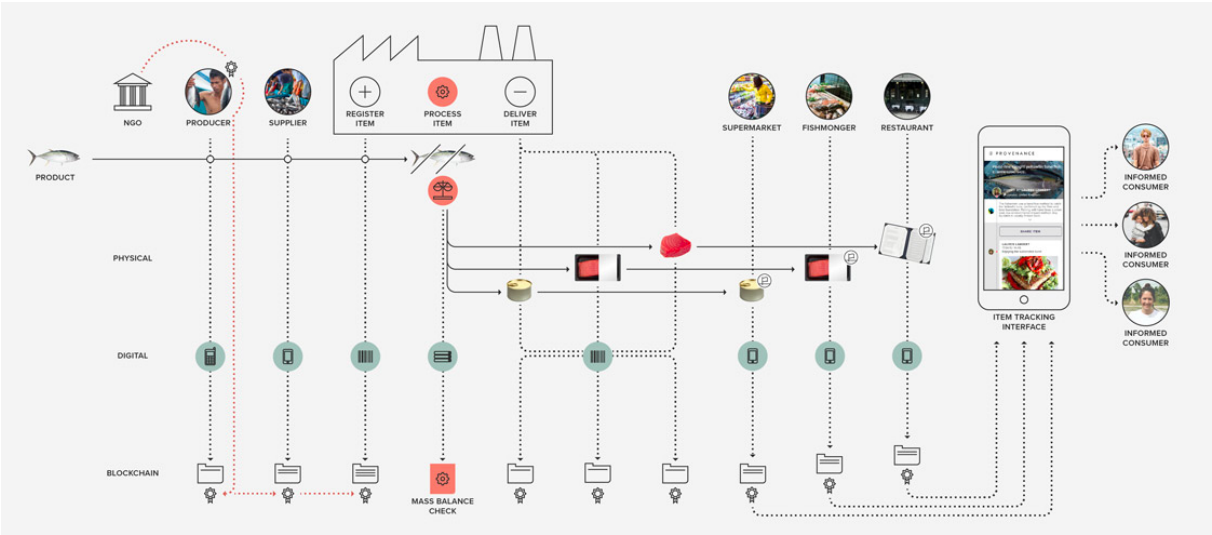

Figure 16- Layer of truth provided by Blockchain accross the supply chain (Source: https://www.provenance.org/tracking-tuna-on-the-blockchain)

4.7 KEY CHALLENGES FOR PROVENANCE

Just to be clear, it's better to make some clarifications about key points of the projects, that Provenance itself wants to specify in describing the project.

First, the choice of using a public blockchain rather than a private blockchain has specific motivations. In fact for Provenance it would be easier to build a private blockchain in terms of cost and feasibility, but they believe that the complexity of using a public blockchain is worth all the effort in terms of transparency.

As said in the first chapters, using a public blockchain ensures points of strength that are the equality, since anyone can join it without special requirement, Consensus and Network effect.

In the pilot project the hypothesis is to use the public blockchain, and Provenance is working towards building the standard and extend this protocol, in collaboration with other industry experts.

Another point that should be clear reading the description of the project is that one of the main goal of Provenance is to guarantee the interoperability of data between blockchain and existing systems, like ERP, SAP or other data management systems.
In fact, supply chain management solutions for managing data and information already exist, but they are expensive or run on private and exclusively internal hardwares; basically they are unable to cover a complete product's supply chain or catching the very first instants of the products. The main reason is that currently they refuse interoperability and open standards, in fact open standards could enable the communication between not-connected systems through a single language, single structures and identifiers.
This is fundamental for companies that could join Blockchain with their own systems and have access or import all the relevant information. Anyway this is still something not realized, and Provenance is working towards this direction: developing a community-owned, open standard, interoperable by definition, since any entity is able to access information and data about a particular product and, the system they use to do this, becomes irrelevant. Blockchain should constitute a first and base layer of truth for material products.

The last key point is a technical issue regarding more the technologies used as products' identifiers than blockchain technology itself. In the project development Provenance hypothesizes the use of QR codes, NFC tickets, etc. but they can be easily copyable.
Other optimal solutions could be bubble tags, nano spirals technology, etc., suitable mainly for high-value products, and Provenance is working with hardware partners to develop the optimal solution at an absolute level.

4.8 POINTS OF STRENGTH OF BLOCKCHAIN COMPARING TO TRADITIONAL METHODS

Today, without blockchain, tuna fish supply chain's actors are using traditional methods like digital labelling, Excel files and reporting, can printing, ipad data collection, but also pen and paper accounting of materials going in and out the facilities, managed by organizations, NGOs, Indonesian companies, etc.

As stated in the first chapter, today's centralized information systems, managed by third parties, have been always the unique way to achieve transparency but considering a single NGO, Association or Institution as the only responsible for transparency means also admitting that there is a single point of failure in the system. And the problem in these specific supply chains, comparable to many others, is that who is the greatest traceability provider may gain great monopolistic power, paradoxical and unsustainable for a pool of actors organized in a network.

The project, thanks to blockchain technology, tries to store data in an immutable, decentralized and distributed, globally-reachable ledger that, by definition, is able to protect identities and can be verified in every moment.

What emerges from the description of the project is that companies approaching to blockchain technology should consider that it's important to start using it and that it may be completely compatible with other initiatives or projects aimed at the same goal already in place, because it may constitute a unique backend with a common language and a shared infrastructure fundamental to support the way towards the total transparency.

As one of the promises of blockchain technology, using it implies greater inclusion, benefits and profit for all the actors in the network, including people in developing economies, providing an underlying layer with incentives and data sharing that supports the fishermen as well as customers as well as companies that use their brands on packages. Once all actors in the network understand the potential of acting in this way rather than catching oligopolistic power, blockchain technology may become an open standard.

Let's see in concrete what Blockchain technology is able to ensure that current traditional methods are not:

- High reliability, availability and quality of information granted

  Information on blockchain is completely reliable, durable and immutable thanks to blockchain infrastructure itself; specifically, information like data and time of transaction, location and ownership is added automatically, correctly and timely, contextually with real transactions, using smart contracts, open source protocol and private and public keys, and once added it is permanently recorded and visible. Since it's an open platform, a consumer in Italy or in US feels free and able to consult everything about tuna eaten at the restaurant, without special requests or permits. Surely, now that data and information are responsibility of single organizations or institutions and actors are geographically and culturally distant, people feel unsure and unconfident about who, when and how information have been released in the system. Other unpleasent consequences due to traditional methods of collecting data are the risks that devices that store them may be hacked, shut down, broken and consequently data may be damaged, modified, frauded or lost.

- Less friction due to paperworks in the supply chain

  For instance, Indonesian companies involved in the project stated that they use methods like excel reporting, pen and paper accounting, ipad data collections, etc. and then, after collection and organization of data, send them via mail to connect them with the ones of other companies; this implies, first, large friction in the process and, then, higher risk of losing or damaging data. If only eight companies send hundreds of files of data, maybe with different software and formats, how frictionless could be the process? How much delay can working with paperwork cause? While with blockchain, collecting data and information appears as a more standard, automatic and effortless process.

- More and better transparency especially upstream of the supply chain

  Today, without blockchain, lack of transparency is a vivid problem along the whole chain, but especially upstream; a customer that buys a tuna can in Italy should make a great effort to find information about that product, for example

the name and certifications of fishermen, as well as other information upstream of the supply chain.

With initiatives of this kind, customers feel more aware in their buying process to choose "positive" products, in terms of quality and production practices, companies and distributors feel safer since their reputation may be deeply nicked in case of not monitored bad events, but what is interesting about the project pilot is that it takes into account needs and problems of the community of fishermen in Indonesia, the very first suppliers of the chain.

The project shows how fishermen acquire a clear identity and greater consideration in front of other partners downstream; consumers and retailers can have a more "direct" contact and linkage to fishermen and for instance they become able to distinguish products of high quality, produced according to standards and "green" practices from the others.

- Better identification of frauds, issues and bottlenecks

  With several systems and methods that collect data in a disconnected, dispersed and frictional way, it's unlikely that actors have a clear vision of what happen allong the supply chain and identify the points of origin of the problems, in terms of overfishing practices, human right violation, unregulated and unreported fishing but also issues of inventory management, delays or errors in production and shipping; while with blockchain, issues and problems, and consequently solutions, are more tempestively and better tracked and identified.

The development of this project incorporates the main trends that are driving the diffusion and adoption of blockchain technology and it could represent one of the first "off-road" projects that applies blockchain to industries, other than financial one; it may be taken as example by other companies, just think that Provenance itself is collaborating with many major enterprises, for example the retailer hiSbe Food CIC and other retailers of Europe or US, that could develop in turn their projects, enlarging the network effect of the technology.

The project, beyond the specific aim of improving transparency along the supply chain, is aimed to pursue of efficiency and profit, as a company operating in the business field,

and this seems to be a really shared and desirable goal to be achieved by all the actors involved in the project.
Consultants and researchers are studying all the projects using blockchain technology and find some characteristics that define the main trend followed by the companies; Provenance's project is a clear example of how Provenance combines a clear vision towards commercialization, a push towards standardization of "technology, processes and skill-sets" and hard work to guarantee the interoperability between different systems.

4.9 LIMITS OF THE PROJECT

Despite Provenance showed how they manage to build a platform ensuring 360° transparency in theory, the project has some limits and weaknesses that, for now, are hindering the application of it in the market.
Beyond the general limits of blockchain technology as it is, described in the previous chapter, the specific obstacles that emerge in this project are:

- Technological paradox: very sophisticated technology for not technology-sophisticated users.
- Blockchain not interoperable and discouraging open standards
- Initial reluctance towards cooperation in the network

First, beyond blockchain technology, Provenance uses a technology to enable the identification and connection between products and devices that includes 2D technologies, like NFC tagging, QR coding, smart tickets, etc. and the team itself sustains that, although these are technologies more advanced than the ones used today in Indonesia, it's not enough considering issues of security.
In fact they are working hard with technology and hardware partners to find other suitable solutions, they will use different technologies for different categories of products, dividing high value products from low value products. While for low value products 2d technologies are enough, for high value products they are developing solutions ad-hoc, like bubble-tags, nano technology, etc.
Anyway, the paradox is that Provenance continues to develop and use a more and more sophisticated technology, but it's not completely sure that the actors on the network,

especially suppliers and manufacturers upstream in Indonesia or in the developing world, have access or are ready to use them.

From a first research phase, the team found that, even if they mainly use old-fashioned and surpassed methods, Indonesian companies and actors have a working mobile phone and have access to 3G or wifi connection, although patchy. Actually this seems true; in Indonesia smartphone ownership is increasing, considering that between 2014 and 2017 the percentage rose from around 30% to 40%.

Furthermore, as stated in the previous chapters, blockchain technology at the current state is not very user-friendly, considering that websites and interfaces present difficult data, difficult interaction for someone not used for this kind of experience; in its business plan, Provenance has already taken into account this issue, so that they develop their personal platform with a simple and immediate design and functioning, with interaction with other platforms used to track products and connect data.

Anyway these data are not very reassuring and the technological issues remain something to be resolved to make the project efficient at its most, considering that these avant-garding technologies are very sophisticated and require confident users to be used in the right way.

Then, what Provenance team is particularly worried about, is the interoperability of the system with the already existing ones; in fact their idea is to build an infrastructure on blockchain that dialogues with existing systems and initiatives, more than developing a completely new and disruptive system.

Surely systems that now work in the supply chain management system have some inefficiencies; for example the fact that they are expensive, run on private hardware or clouds, or are unable to track all the informations from the first step.

The aim of Provenance is to define open traceability standards that guarantee interoperability between blockchain and old systems, in which blockchain constitutes a common layer of truth in the product world; in particular they believe that the unique ID that corresponds to an address on blockchain, accessible to every actor dealing with the product, interoperable by definition since data are accessible in different ways and importable to other (more common) systems, may constitute the next ideal standard in the supply chain management systems.

There is already a set of few global standards in act, for example GS1, an NGO, manages a set of global standards like ID keys, RFID and barcodes, but really different from the idea that Provenance has of a community-owned, open standard of traceability.
For the same reason, Provenance is determined in using public blockchain, rather than a private blockchain, to ensure transparency, secureness and decentralization at their best and Provenance tries to find industry experts able to help it in building this infrastructure a standard and open source project; using a private blockchain built ad hoc by a consortium may be easier and cheaper but it couldn't ensure the total equality and consensus in the network.
Although this project represents an important milestone in the right direction and many other consortia and initiatives are aimed at this, researchers and experts believe it may be still too soon to think about that, since there is much work to do about the technology itself and its applications.
FInally, one last possible limit to successful implementation of the project may be the initial reluctant and "hostile" attitude of actors in the network to approach this new method of coordination and to change accordingly to this new infrastructure. Companies and businesses have always consider pursuit of profit and revenues as their first objective and consequently they don't consider efforts toward transparency strictly necessary, but now that "green" practices and standards are acquiring greater and greater importance and transparency is becoming a source of competitive advantage over others, their attitude should change. Obviously moving from a centralized system to a decentralized one require a behavioural change of actors involved, since, as described before, rules, features and characteristics change drastically. Until major enterprises, companies and businesses don't understand clearly and totally the importance of pursuing transparency as primary goal and the potential of blockchain technology, projects like tuna pilot project of Provenance risk of not being reliable.

4.10 HOW BLOCKCHAIN CHANGES TRANSACTIONS THE NETWORK

Now that a concrete and tangible project has been described, it should be more clear how blockchain works in practice and how transactions and exchanges are changed accordingly.

In the first chapter, concepts that have always characterized transactions like trust and social embeddedness are described and analyzed; now it's time to see how these features have been changed by this disruptive technology, together with other ones like information, role of the actors and reputation.

First, as it's clear from the project, blockchain technology is able to create linkages between the actors operating in the supply chain, creating a form of network, that covers a large portion of the global surface. And these actors are really dispersed, diversified and with different background and different expectations, from fishermen in Indonesia to retailers in UK, US or Japan to final consumers all over the world.

As described in depth in the first chapter, in the network, one of the most important mechanism of coordination has been trust based on cognitive and relational aspects, that creates embedded relationships, since the first value exchanges. This may be a perfect infrastructure to ensure transparency between business actors. With globalization and digitalization, supply chain expanded more and more, and actors need alternative coordination mechanisms that don't require inevitably strict personal contact, building relationships or trust.

In fact, nowadays, to ensure a satisfactory level of transparency, transactions require someone able to control and monitor the situations, as in the market paradigm; in this "trustful" culture, intermediaries and third parties are inevitable.

Blockchain technology may disrupt this paradigm, leading to a "trustless" culture, in which "trust" is a fundamental coordination mechanism imposed by technology itself by definition, without relying neither on personal relationships nor on intermediaries or third parties.

But let's see how blockchain has changed the nature of transactions, in particular considering how it may disrupt coordination mechanisms in the network and the features connected to this, as evident in this case study.

To give an idea of which is the ideal coordination mechanism in network on blockchain, this may be considered the "trust", intended as the one created by technology, and the coordination of intentions and attitudes of the actors.

First, in the blockchain network, "trust" is imposed just by the technology, a completely innovative concept, thanks to cryptography and use of public and private keys, as described in detail in the second chapter.

In fact in the case study, actors involved inevitably have little real personal trust in each other because they personally don't know each other and share nothing, but the scope. Basically considering this, it results that the transactions are quite "impersonal", for the fact that the parties have no direct and tangible contact most of the times, and happen through mechanisms, the smart contracts, comparable to classical contracts, but more automatized and objective.

Then, as in the network coordinated by social embeddedness, self-interest of people, intended as the self-interest in managing the network, plays a primary role, so in the network on blockchain "self-interest" in running the network securely has the same relevance. In fact a key point about coordination on blockchain is that it seems to work with the rule that if you want to succeed, you have to play by the rules of the system itself. Since the network is made of different, distributed and diversified stakeholders, they should understand which is the goal of the network and adequate their intentions, efforts and attitudes accordingly. Basically, technical features of blockchain, including consensus mechanism or cryptography, make all nodes work together and feel the same responsibility of making the network work.

Regarding information sharing, since the most remote years in market-like paradigm price is the only information that counts, in fact parties have always relied on price to decide whether a transaction is achievable or not. Transactions on blockchain work in a different way in fact parties expect to get all the information, quantitative but overall qualitative, from time and date of transactions, names of the actors, certifications about tuna fish, concerning the product before realizing definitely the exchange. Nowadays actors in the supply chains don't buy by force the product or raw material that cost less, but they are also willing to pay more for a product that respects certain conditions and standards, that are proven to be of high quality and certified all along the chain. This is why sharing large amounts of information is acquiring great importance in the value transactions. As shown in the project, actors that have to decide whether to buy or not, interacts with the interface and expects to find all the possible information concerning tuna and even the previous owners, including the fisherman. Quality of information may be influenced by reputation of the actors, anyway blockchain technology is thought to provide a great level of certainty and reliability of information.

Regarding problem solving arrangements, it may be more facilitated using blockchain technology, given the overall vision that actors may have over the supply chain; it may

speed up decision making and make it more collaborative and more synchronized. Just think, for example that if the supplier ships to the manufacturer only 480 tuna and not 600 as expected, this is completely visible to everyone and first, everyone is able to verify if it has been a question of bad intentions or for example a technical problem, then it's possible to find an immediate corrective solution. In this way decision making is facilitated, because actors are able to view "the big picture" across the whole supply chain, analyzing and considering reliable and up-to-date data and information.

As Uzzi described (1996), in embedded ties problem solving arrangements are described as collaborative actions that intensify the personal relationships between actors and that rely on the expectation that everyone acts in good faith on the base of these relationships; in blockchain network, problem solving works as a "collaborative" effort aimed to guarantee the efficiency of the system, but problem solving decisions are taken on objective, certain and completely reliable information.

Also on blockchain, reputation of individuals counts; since every actor in the real world corresponds to an "identity" on blockchain, once these profiles are visited, people are able to see which certifications they have, how much productive a fisherman is, how sustainable the manufacturer of tuna is, etc. It should be clear that reputations on blockchain are based on objective, past and verifiable data; in the project actors decide whether relying on one actor or not considering what emerges from his profile on blockchain, that records everything happened in the previous transactions. Reputation plays not a primary role in information sharing, but rather precisely in classifying and evaluating partners. Blockchain acts as a form of "personal referral", since the technology itself acts as a guarantor of someone in the network.

CONCLUSIONS

By definition, Blockchain Technology is considered a shared, public and immutable "ledger", which enables actors in the network to access data in a decentralized and trustless way.

What fundamental emerges describing its functioning is that just by design it is able to provide to users key advantages like transparency, authenticity, security and immutability; this explains why blockchain has many different applications beyond the financial sector and the payment system, and one of the most interesting is the application to supply chains.

Today the need of transparency in supply chains is vivid as never before because actors are geographically and culturally distant and dispersed, products are chosen for their authenticity, genuineness and high quality, and "green" practices and Standards are more and more relevant; without blockchain, information flow is managed centrally by NGOS, organizations, third parties, with traditional and not efficient methods.

By design, blockchain is able to provide a base layer of truth about products, a common backend beyond existing initiatives and systems, to support the growth of a new standard for traceability; the project shows how blockchain enables information reliability about transactions and identities, total transparency especially upstream and better and efficient monitoring of operations.

The project highlights how blockchain enables all actors in the network to have direct control over their information and data, without intermediation, and potentially gain profit from this; the evident problems of exploitation and fraud in developing economies are only the trigger, but all the actors benefit of connected, secure and open information. In fact suppliers upstream acquire greater consideration, producers and partners are more aware about day-by-day operations, goods acquire an added value and purchasing decisions become smarter; items, products, raw materials, people obtain an identity on the digital, open blockchain platform, that are updated automatically.

This is possible because blockchain technology is able to introduce trust just by design, thanks to combination of cryptography, informatics and mathematics, automated smart contracts, identities authentication and public and private keys. Considering that before, in the "trustful" culture, or trust was generated naturally by social and cognitive interaction or intermediaries obviated the issue with monitoring and contracts, it's

obviously a great advantage to have trust intrinsic and set directly by technological infrastructure. With blockchain technology, actors of the supply chain constitute a network whose coordination and trust mechanisms that rule transactions are set by blockchain structure itself, just for how it has been developed from a technical point of view.

Major Companies and start-ups are developing projects similar to the one described to exploit blockchain potential and to enhance metrics and performance indicators but, even if advantages of such a technology seem obvious, its adoption is slowed down by both technical and not-technical challenges; the debate whether blockchain-based applications are applicable and profitable or not is vivid at most at the moment.

Beyond technical limits, one important challenge to overcome to enable further diffusion and adoption is the bad reputation that blockchain has acquired being associated to cryptocurrencies, but all along the elaborate it's clear that, although born contextually, they are two distinct phenomena.

It's fundamental to understand that, until people and users are skeptical about this disruptive innovation, its potential can't be exploited at best; in fact blockchain technology would need a regulation framework, or more correctly a good leadership, provided by people involved with a positive and collaborative behavioural attitude.

Until people don't understand clearly the benefits of blockchain technology and don't perceive them as incentives to be transparent, it's difficult that blockchain technology development is not slowed down.

FInally, it's too early to know what the fate of blockchain will be, anyway it's clear that it is a definitely interesting and controversial phenomenon to keep under control; although adoption and diffusion of blockchain technology is quite slow at the moment considering people being skeptical because of associated limits and risks, it's quite likely that soon blockchain potential will fully understood and applied to interesting projects across all the industries.

REFERENCES:

- Anon, (2016). *A gentle introduction to smart contracts*. [online] Available at: https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smartcontracts/ [Accessed 10 Nov. 2017].
- Antonopoulos, A. (2017). *Mastering bitcoin*. Sebastopol, CA: O'Reilly.
- Baker, J. (2016). Trust in the Digital Age. [online] Available at: https://www.provenance.org/news/movement/trust-digital-age [Accessed 15 Jan. 2018].
- Bank of England (2015). The economics of digital currencies. [online] Available at:https://www.bankofengland.co.uk//media/boe/files/digitalCURRENCIES/the-economics-of-digital-currencies [Accessed 9 Dec. 2017].
- Blockchain Unleashed: IBM Blockchain Blog. (n.d.). [online] Available at: https://www.ibm.com/blogs/blockchain/ [Accessed 8 Nov. 2017].
- Deimel, M., Frentrup, M. and Theuvsen, L. (2008). *Transparency in food supply chains: empirical results from German pig and dairy production*. [online] Available at:http://www.wageningenacademic.com/doi/pdf/10.3920/JCNS2008.x086[Accessed 25 Sep. 2017].
- Deloitte (2014). *http://www.deloitte.co.uk/makeconnections/assets/pdf/path-to-supply-chain- transparency.pdf.*[online] Available at: http://www.deloitte.co.uk/makeconnections/assets/pdf/path-to-supply-chain transparency.pdf [Accessed 29 Oct. 2017].
- Deloitte (2017). Blockchain to blockchains: Broad adoption and integration enter the realm of the possible.[online]Available at: https://www2.deloitte.com/insights/us/en/focus/techtrends/2018/blockchain-integration-smart-contracts.html [Accessed 1 Jan. 2018].
- Demirors, M. (2017). Women in Blockchain: Jessi Baker @ Provenance. [Blog] Medium. Available at: https://insights.dcg.co/women-in-blockchain-jessi-baker-provenance-67c70330d9a7 [Accessed 17 Jan. 2018].
- Frentrup, M. and Theuvsen, L. (2006). *Transparency in Supply Chains: Is Trust a LimitingFactor?*. [online] Available at: http://ageconsearch.umn.edu/bitstream/7733/1/ sp06fr01.pdf [Accessed 21 Oct. 2017].
- GitHub. (2017). [online] Available at: https://github.com/ethereum/wiki/wiki/White-Paper [Accessed 15 Nov. 2017].
- Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. American Journal of Sociology. [online] pp.481-510. Available at:

https://sociology.stanford.edu/sites/default/files/publications/economic_action_and_social_structure.pdf [Accessed 29 Oct. 2017].

- Hackett, R. (2017). Blockchain mania. Fortune.
- Hofstede, G. (2003). *Transparency in Netchains*. [online] Available at: http://www.informatique- agricole.org/download/efita-conference/Congres_EFITA_2003/0003.pdf [Accessed 29 Oct. 2017].
- Hofstede, G. (2003). *Trust and transparency in supply netchains: A contradiction?*.
- Hofstede, G., Schepers, H., Spaans-Dijkstra, L., Trienekens, J. and Beulens, A. (2004). *Hide or confide? The dilemma of transparency*.
- IBM (2016). *Trust in trade*.[online] Available at: https://www-01.ibm.com /common/ssi/cgi-bin/ssialias?htmlfid=GBE03771USEN& [Accessed 29 Oct. 2017]
- International Pole & Line Foundation (2016). Pole-and-Line Tuna Fishing in the World: Status and Trends. [online] Available at: http://ipnlf.org/perch/resources/ipnlf-tech-report6status-and-trends-of-pole-and-line-tuna-fishing.pdf [Accessed 13 Jan. 2018].
- Jayachandran, P. (2017). *The difference between public and private blockchain*. [online] Available at: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ [Accessed 7 Nov. 2017].
- Loughborough University, UK (2016). *Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger*. [online] Available at: https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/22625/1/Monfared-BCReady%20Sept%2016%20Lboro.pdf [Accessed 19 Oct. 2017].
- Meola, A. (2017). The growing list of applications and use cases of blockchain technology in business & life. *Business Insider*. [online] Available at: http://www.businessinsider.com/blockchain-technology-applications-use-cases-2017-9?IR=T [Accessed 11 Nov. 2017].
- Needham (2015). The Blockchain report: welcome to the internet of value. [online] Available at: http://www.the-blockchain.com/docs/The%20Blockchain%20Report%20-%20Needham%20(Huge%20report).pdf [Accessed 4 Dec.2017].
- Oracle (2010). *The Fragmented Supply Chain*. [online] Available at: https://www.themanufacturer.com/mdc2011/pdf/ChainReaction-The-Fragmented-Supply-Chain.pdf [Accessed 28 Sep. 2017].
- Oxford Dictionaries | English. (n.d.). [online] Available at: https://en.oxforddictionaries.com/definition/cryptocurrency [Accessed 10 Nov. 2017].

- Perez, Y. (2015). How Provenance is Channeling the Blockchain for Social Good. [online] Available at: https://www.coindesk.com/provenance-channeling-blockchain-social-good/ [Accessed 16 Jan. 2018].

- Peterson, B. (2017). IBM wants to use the technology that underlies bitcoin to help prevent major foodborne outbreaks like salmonella. *Business Insider*. [online] Available at: http://www.businessinsider.com/ibm-and-walmart-are-using-blockchain-in-the-food-supply-chain-2017-8?IR=T[Accessed 29 Oct. 2017].

- Podolny, J. and Page, K. (1998). Network forms of organization. [online] Available at:https://www.researchgate.net/publication/228589195_Network_Forms_of_Organization [Accessed 15 Jan. 2018].

- Prisco, G. (2017). Deloitte's 2018 Outlook Highlights the Growth of Blockchain Technology. [online] Available at: https://distributed.com/news/deloittes-2018-outlook-highlights-growth- blockchain-technology/ [Accessed 10 Dec. 2017].

- Provenance (2015). *Blockchain: the solution for transparency in product supply chains*. [online] Available at: https://www.provenance.org/whitepaper [Accessed 18 Oct. 2017].

- Provenance (2016). From shore to plate: Tracking tuna on the blockchain. [online] Available at: https://www.provenance.org/tracking-tuna-on-the-blockchain [Accessed 10 Jan. 2018].

- Provenance (2016). The Story Behind the Tuna. [online] Available at: https://www.provenance.org/news/technology/story-behind-tuna [Accessed 17 Jan. 2018].

- PwC (2016). Tech breakthroughs megatrend. [online] Available at: https://www.pwc.com/gx/en/issues/technology/tech-breakthroughsmegatrend.pdf [Accessed 14 Dec. 2017].

- Salmonella outbreak linked to Mexican papaya sickens more than 100 in US. (2017). *The Guardian*. [online] Available at: https://www.theguardian.com/world/2017/aug/08/salmonella-outbreak-papaya-mexico-consumer-warning [Accessed 29 Oct. 2017].

- Statista. (2018). Number of mobile phone users in Indonesia from 2013 to 2019 (in millions). [online] Available at: https://www.statista.com/statistics/274659/forecast-of-mobile-phone-users-in-indonesia/ [Accessed 14 Jan. 2018].

- Sustainable Fisheries Partnership (2011). Sustainable Indonesian Tuna Initiative White paper. [online] Available at: http://cmsdevelopment.sustainablefish.org.s3.amazonaws.com/2011/12/19/Indonesia_Tuna_white_paper_dec2011-4935d05c.pdf [Accessed 13 Jan. 2018].

- Tapscott, D. and Tapscott, A. (2016). *Blockchain revolution*. [Place of publication not identified]: Portfolio Penguin.
- Topham, G., Clarke, S., Levett, C., Scruton, P. and Fidler, M. (2015). The Volkswagen emissions scandal explained. *The Guardian*. [online] Available at: https://www.theguardian.com/business/ng-interactive/2015/sep/23/volkswagen-emissions-scandal-explained-diesel-cars [Accessed 17 Sep. 2017].
- Uzzi, B. (1996). *The sources and consequences of embeddedness for the economic performance of organizations: The network effect*. [online] Available at: http://www.kellogg.northwestern.edu/faculty/uzzi/ftp/sources.pdf [Accessed 12 Jan. 2018].
- Uzzi, B. (1997). Social structure and competition in inter-firm networks: The paradox of embeddedness.