UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Tecnica e Gestione dei Sistemi Industriali
Corso di laurea in Ingegneria Gestionale

Tesi di Laurea Magistrale

Applications of Blockchain Technology in International Logistics - a Case Study

Relatore *Roberto Panizzolo*

Laureando *Riccardo Caneve*

Anno Accademico 2017-2018

Abstract

The aim of this work is to give some insights about the beneficial impact that blockchain technology could have on the trust paradigm of modern supply chains, especially in the international logistics sector.

The elaborate is divided into three main parts. In the first one (Chapter 1), a non-technical but detailed description of how the Bitcoin protocol works will be given. It is worth noting that the aim of the project is not to make the reader an expert in the field of blockchain and decentralized technologies. However, some explanations are needed in order to properly understand concepts like the security model and the fault-tolerant nature of this new protocol, which will be central arguments in favor of blockchain technology.

In the second part (Chapters 2 and 3), the focus will shift on the possible applications of blockchain technology in the logistics industry, highlighting some notable pilot project already implemented and a possible classification of the solution which the ecosystem is developing towards.

The third part (Chapters 4 and 5) will be reserved for the case study, theorized with the support of Luxottica. A summary of the company's history and main strengths will be followed by a description of how the process of a container shipment is structured nowadays. Finally, a complete description of the new process, structured using a distributed ledger as a backbone, will be formulated. Every step of the flow will be analyzed and the benefits of blockchain underlined. In order to measure the improvements such a re-designed process could bring to the company its performance will be evaluated on a set of criteria which have a critical importance for Luxottica.

Summary

Introduction

Transparency has been one of the key elements of every business relation since the birth of human commerce. However, with the globalization and internalization of supply chains it has become more and more difficult and expensive for companies to maintain visibility over the network's participants and flows. In order to maintain the desired level of trust, significant inefficiencies have to be tolerated and intermediaries have to be paid.

The term *blockchain* was born in 2008 as a definition for the underlying database of the first and most famous cryptocurrency, Bitcoin. Although the concepts of blockchain and digital currencies are tightly correlated, the two seem to follow different innovation paths. In fact, it is now clear that this new paradigm is well suited to revolutionize not only the financial sector, but a broad spectrum of markets ranging from the insurance industry to the healthcare and energy ones.

According to Seppälä, the possible uses of this technology cover "any sort of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property) and intangible assets (votes, ideas, reputation, intention, health data, information, etc)" (Seppälä, 2016).

The term has been at the center of a mediatic hype in the recent months. The total market capitalization of the available cryptocurrencies rose from only $10 billions at the beginning of 2017, to more than $800 billions in December of the same year. Venture investments in blockchain-related startups have soared as well, trying to ride what could be defined a "maniac" trend. Pilot projects started to be launched also by important enterprises, like IBM or Maersk.

But while many described blockchain as a possible solution for almost every aspect of human interactions, others (like Jamie Dimon, J.P. Morgan's

CEO) expressed their absolute antipathy for what Bitcoin could bring to the world. Therefore, one of the purposes of this work will be to give an objective and factful description of what is currently achievable with this technology, which are the main threats and the available solutions.

The thesis conceptualization and creation were part of an internship done in Luxottica, an Italian multinational company currently leader in the eyewear and sunglasses industry. Particularly, the experience was conducted in the logistics department of the Oakley AFA business unit, responsible for the shipment of the apparel products of the notorious American brand. The company confirmed its interest towards the new technology and its possible logistics applications and gave precious insights on the main inefficiencies as well as drivers for a process improvement.

Chapter 1 – Blockchain Technology

1.1 Introduction

In this chapter we are going to examine the core technological elements that make Bitcoin such a ground-breaking innovation that will change the way we exchange value on the internet, from money applications to supply chain and logistics ones. The aim of the following technical introduction is not to make the reader an expert in the field of distributed ledger technology but to justify, in the clearest and simplest way possible, how it is possible to state that blockchain technology grants more security, immutability and transparency than modern centralized information systems.

Even though the concept of blockchain goes well beyond any single cryptocurrency project, the Bitcoin protocol has been undoubtedly the conceptual foundation of the entire ecosystem. We will therefore take Bitcoin as a reference for the following analysis of the technology behind blockchain.

All the features and benefits of blockchain technology, such as transparency, immutability and censorship-resistance, derive from a simple but powerful set of mechanisms and inventions that were theorized well before Bitcoin's idea was published by the anonymous Satoshi Nakamoto, in late 2008.

E-cash was invented by David Chaum in 1983, as one of the first notable attempts of an anonymous electronic currency, which took advantage of public key digital signature schemes (D. Chaum, 1983). Every coin was cryptographically signed by a bank, ensuring its value. People could spend and exchange E-cash with Vendors in a peer to peer and totally anonymous way, and then redeem the fiat currency at any time.

Hashcash's aim, proposed in 1997, was to create an email protocol which could resist to spam and denial-of-service (DoS) attacks. Its creator Adam Back intelligently used a proof-of-work system to achieve his goal. In a way similar to Bitcoin's proof of work algorithm, which we'll see in depth later, senders using Hashcash were required to generate a valid header for their messages. Finding a valid header took time, because the only way possible was through brute force iteration, until a valid one was found; on the other side, verifying the correctness of this header was immediate for receivers, that could mark emails with such a valid title as legitimate and the others as spam (A. Back, 2002).

Another interesting project was *B-money*, also referenced in the Nakamoto's 2008 whitepaper. The idea was published by Wei Dai, its founder, on the famous *cypherpunks* mailing list in 1998. It was essentially the first theoretical implementation of Hashcash's proof-of-work algorithm for digital money purposes. Dai also envisioned the possibility of programming some basic smart contracts logics on B-money, but never created a practical version of his proposal.

The *Bit Gold* project, proposed by Nick Szabo in 2005, was arguably one of the closest to Bitcoin's protocol. Szabo imagined a way to produce scarce proofs-of-work that would therefore have an intrinsic value and link them to the creator's public key. All these digital assets were chained to one another, maintaining a global consensus on the chronological order and thus preventing double spending attacks (N. Szabo, 2005). Szabo also projected the possibility of pairing the assets with real life properties, such as domain names or even physical possessions.

The elegance of the Nakamoto paper, published on October 31st, 2008, resides in the fact that he was able to condensate the work of his precursors in an elegant and incredibly powerful protocol. He introduced the idea as "A purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution" (S. Nakamoto, 2008).

1.2 Blockchain definition

The term “blockchain” appeared for the first time in 2008, as the database structure chosen for the implementation of the Bitcoin protocol. Essentially, it can be defined as a “chronological chain of blocks” (see a graphical example in Figure 1.1) where each one is destined to contain a “record of valid network activity since the last block was added to the chain” (Needham & Company, LLC, 2015).

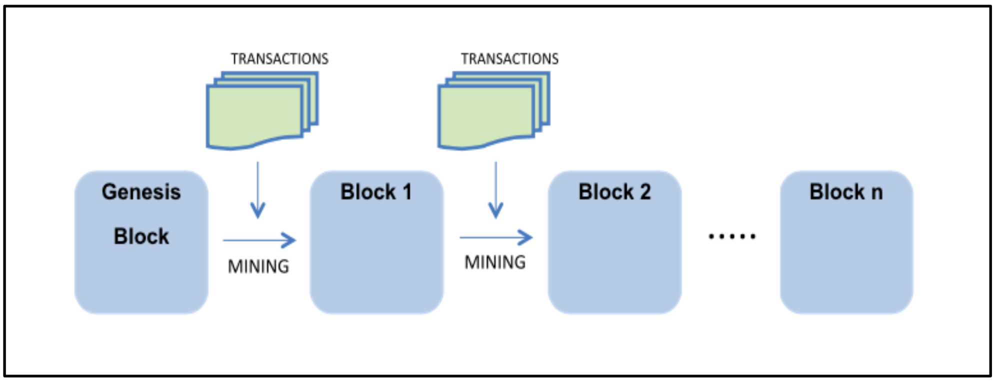


Figure 1.1: A Blockchain seen as a chronological series of linked blocks (Needham & Company, LLC, 2015).

Every transaction first has to be propagated to the network. All the nodes will then validate and add it to the next block on the chain, giving the recipient the confirmation that the associated funds can be spent.

While reading the blockchain is immediate, because it’s shared with all the peers, changing it is practically impossible. Once a transaction is included in a valid block, and the block has a sufficient number of followers in the chain, deleting or modifying it is impossible. This important feature removes the need for any central authority that has any intermediary role, because the peers can autonomously verify each movement and ensure that no one can fraud the system.

The network is completely open, and any node can freely leave and join it whenever it wants. The incentive for participating and sustaining it comes from the rewards that special nodes, called “miners”, get for the computational effort they provide.

The main features of any blockchain, not only Bitcoin’s one, are:

- *Decentralized and distributed consensus*: as stressed before, “decentralized” means that there’s no single point of failure in the system. Even if 99% of the nodes turn off at the same time, the remaining 1% would have no problem in keeping the network up and running. Moreover, when the nodes would come back online, they would be able to immediately agree on the past transaction history (achieving *consensus*) and proceed from that point. This characteristic makes the system more reliable than any centralized network, which has always a higher risk of malfunctioning or deliberate attack.

- *Public*: although in most of the cases the single addresses (that represent individual nodes) are anonymous, the ledger is always completely transparent. Everyone can check all the transactions happened to the Bitcoin blockchain, back until the first one on January 2009. This feature makes the system essentially *trustless*: nodes don’t need to put trust in any other peer, but only in the network itself and its structural security, which has never been violated until now.

- *Immutable*: as mentioned before, re-writing an event that is tracked on a blockchain is almost impossible. We’ll cover the mining process in depth later, but it’s important to understand that each block is linked to the previous one, so if any actor wants to change one block, he must be able to re-validate all the following blocks for the network to trust the new blockchain he created. This is an incredibly hard task, requiring at least half of the total computational power of the entire Bitcoin network in order to have some chances of succeeding.

- *Encrypted and secure*: it is based on encryption built on private and public keys to keep privacy completely intact. All the incredible features blockchains possess have their foundations in simple but powerful cryptography instruments, that we will cover below.

1.3 Keys and Addresses

Bitcoin was born with the aim of becoming the first real form of electronic workable money. The first aspect of digital money that it was trying to solve was ensuring that the ownership of the assets (in this case, the bitcoins) came with absolute security. That meant that nobody could steal or move them unless he provided the needed authentication key.

As the first part of the word "cryptocurrency" implies, Bitcoin uses cryptography to achieve this objective, declined in two elements we're going to briefly cover: keys and addresses.

1.3.1 Keys

While Visa and other centralized networks typically transmit personal information about their customers (including credit card numbers and passwords) over a channel that has to be secured against external attacks, decentralized cryptocurrencies must encrypt the messages they send, because no one can be excluded from the network, which is open and trustless by design.

The mathematical foundation chosen for the first implementation of the Bitcoin protocol was *Public Key Cryptography* (A. Antonopoulos, 2014). After its conception in the 1970s, many useful instruments and functions have been invented and heavily tested, making public key infrastructure one of the most secure for any application interested in sending authenticated and encrypted messages over an insecure network.

What all these functions share is a very important feature: *practical irreversibility*: it means that, while computing the specific function could be relatively easy, finding the inputs given the final results is possible only through brute force. In other words, it’s impossible (or highly expensive) to find the inverse of the given function (Figure 1.2).

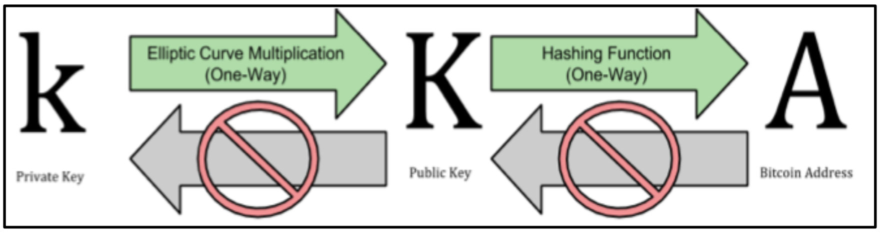
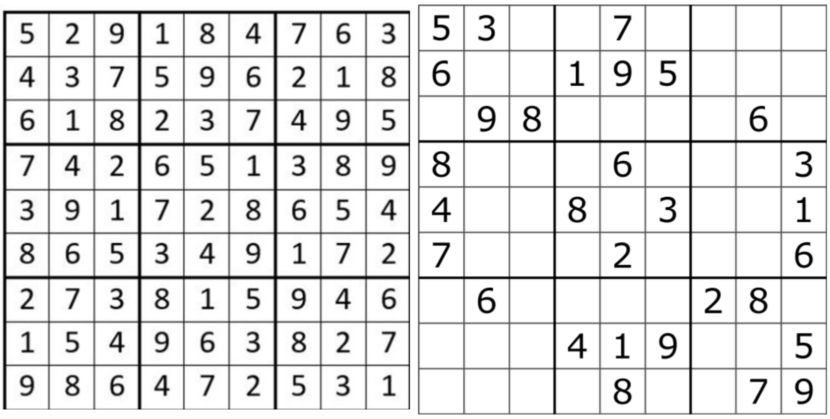


Figure 1.2: relationship between keys and addresses: the concept of irreversibility (Antonopoulos, 2017).

An example, useful to understand this concept, could be a sudoku game (Figure 1.3). In a sudoku table, verifying that a solution is valid isn’t a complex task: all you have to do is check that every row, column and sub-square contains the 9 digits allowed, one time for each digit. While checking the validity of a proposed sudoku solution can be done in under a minute, finding a new solution could take many minutes or hours, depending on the difficulty.



5	2	9	1	8	4	7	6	3
4	3	7	5	9	6	2	1	8
6	1	8	2	3	7	4	9	5
7	4	2	6	5	1	3	8	9
3	9	1	7	2	8	6	5	4
8	6	5	3	4	9	1	7	2
2	7	3	8	1	5	9	4	6
1	5	4	9	6	3	8	2	7
9	8	6	4	7	2	5	3	1

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Figure 1.3: checking the validity of a sudoku game solution is exponentially easier than finding one.

In order to participate in the Bitcoin network, any user has to create a *key pair* that gives him access to an account, capable of receiving and sending bitcoin through the web. The private key can be seen as the PIN code that we have to use to authorize payments. The public key is mathematically derived from the private key and must be shared to other peers that want to send us funds. It can be seen, using the same banking analogy, as our IBAN number.

1.3.2 Private Key

The private key is a random number of 256 binary digits, most of the times represented in 64 hexadecimal digits, like the following one:

1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

As stressed before, this bunch of digits are the centre of all the security model of the Bitcoin network, when it comes to ownership of the funds. It's important to keep this key safe and don't let others see it. Everyone with access to this key can freely move our bitcoins, while the loss of it would cause the complete and irreversible loss of the associated funds.

1.3.3 Public key

The public key of a pair is directly derived from the private one, using one of the aforementioned cryptographical functions: *elliptic curve multiplication*. This mathematical model is based on the discrete logarithm problem and has an important feature: while it allows to easily add and multiply factors, the reverse operator is impossible to find. In this way, finding the initial inputs, knowing the result, requires trying in a brute force and iterative fashion.

The elliptic curve used in the Bitcoin protocol can be visualized in the graph below (Figure 1.4):

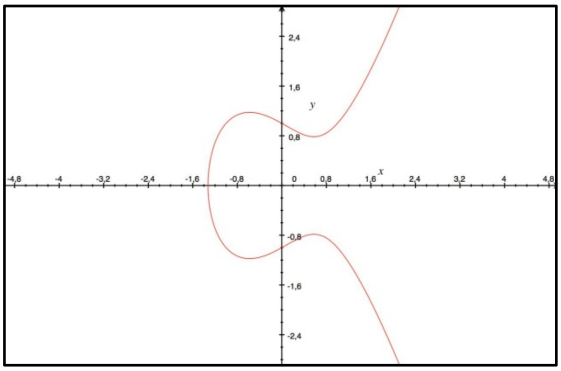


Figure 1.4: an elliptic curve, conceptually similar to the one used in the Bitcoin protocol.

Specifically, the function used in the software is:

$$y^2 = (x^3 + 7)over(\mathbb{F}_p)$$

“$over(\mathbb{F}_p)$” means the curve is defined over a finite field of prime order p, and therefore it consists in a pattern of dots. This mathematics allows for addition and multiplication, in a way similar to the traditional algebraic operations.

Addition can be conceptually explained as follows: given to numbers belonging to the curve, P1 and P2, P3 = P1 + P2 is another point of the elliptic curve, found using the following procedure:

- We trace a line, intersecting both P1 and P2
- This line will intersect the curve in another point, which we will call P3’
- P3 is defined as the symmetrical point of P3’, found reflecting P3’ in the X axis

Multiplication can be defined using the addition operation just explained. As in the traditional theory, the multiplication:

$$P_2 = k * P_1$$

Can be seen as:

$$P_2 = P_1 + P_1 + P_1 + \cdots (k\ times)$$

What it means graphically is the following (Figure 1.5):

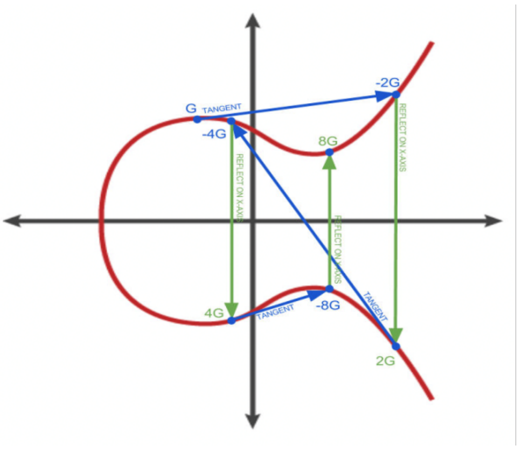


Figure 1.5: Multiplication operator in the elliptic curve domain.

The public key is directly derived from the private key, multiplying it by a Generator Point (G) which is a constant of the Bitcoin protocol.

$$K = k * G$$

As a consequence of the security of asymmetric cryptography, this function is not reversible. In this way, even if G is known and we give others our public key (K), nobody can calculate our private key (k), computing the following equation:

$$k = \frac{K}{G}$$

1.3.4 Addresses

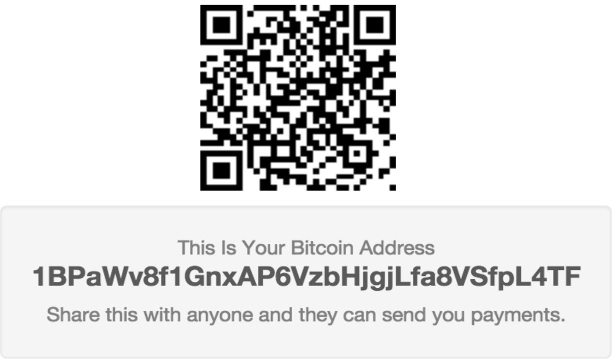
The metaphor of the IBAN representing our public key was in reality not totally accurate. What we share with other peers is in fact not the public key, but the *bitcoin address*. This address can be easily derived from the public key itself, through a series of two hashing functions:

$$A = \text{RIPEMD160}(\text{SHA256}(K))$$

Where SHA256 is a hash function developed by National Security Agency (NSA) of US Government, and RIPEMD160 is a European cryptographic algorithm developed in academic environment.

Given that hashing functions are widely used in the Bitcoin protocol and in general in the cryptocurrency & blockchain space, it’s worth spending some lines defining them: a hashing function essentially maps data into a fixed size format, usually a string of text. The maps are deterministic, so the same inputs will result always in the same hashes, and its execution is most of the times very easy to calculate and not computationally heavy. Hashing functions are adopted in many cryptography applications, because of their infeasibility to be inverted: just like the elliptic curve multiplication, starting from a hash, no-one can obtain the originally input data.

An address can be presented in a special format, called “Base58Check”, which uses all the uppercase and lowercase letters except 0, O, I (capital i), l (lower l) for an easier reading and comprehension (See Figure 1.6).



This Is Your Bitcoin Address

1BPaWv8f1GnxAP6VzbHjgjLfa8VSfpL4TF

Share this with anyone and they can send you payments.

Figure 1.6: a Bitcoin address in its Base58Check format and QR format.

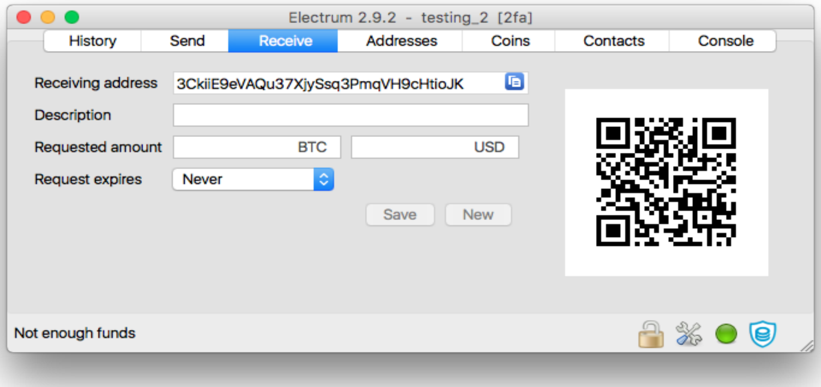
Graphically, the same address can be easily converted in a QR code; many applications take advantage of this function nowadays, because it simplifies the procedure of manually copying and pasting the text string.

Addresses usually represent a public key, owned by a person, but can also be linked to a script. In this case the funds received won’t be tied to a specific private key, which is mandatory in order to later move them, but instead to a script, which will need some special conditions for allowing its value to be transacted. Although Bitcoin doesn’t allow for elaborate smart contract programming (as we’ll see later) this “pay-to-script hash” function can be seen as one of the first moves towards real programmable digital money.

One simple example of a script is the so-called *multi-signature address*; as the term suggests, more than one digital signature are needed in order to move the funds, and different configurations can be easily created (for example M out of N signatures needed, with M < N).

1.4 Wallets

A wallet is simply a software, capable of safely store the key pairs owned by an individual (A. Antonopoulos, 2017). Given the aforementioned attention one has to put on the security of his keys, it seems obvious that some programs and interfaces have been created to make this process more similar to the normal use we make of our passwords. Here’s how a modern wallet looks like (Figure 1.7):



Electrum 2.9.2 - testing_2 [2fa]

Receiving address: 3CkiiE9eVAQu37XjySsq3PmqVH9cHtioJK

Description:

Requested amount: BTC USD

Request expires: Never

Not enough funds

Figure 1.7: home screen of a Bitcoin Wallet (Electrum Wallet screenshot).

Naturally many different wallet types have been created, obtaining trade-offs between the two most critical features such applications must have: *security* and *usability*.

The most secure ones are software wallets that download the entire blockchain locally, like the original Bitcoin Core reference, having complete freedom of verifying each and every transaction by themselves. Computers running this kind of instance are called "full nodes" and are the ones that truly embed the decentralized spirit of the Bitcoin project. They don't need any other node nor have to put trust in any actor, in order to gain consensus on the network status.

As the blockchain steadily grows (nowadays it's about 161 Gb in size, Charts.bitcoin.com, 2018) it becomes harder and harder for a normal pc, let alone a mobile phone, to run a full node. Many web and lightweight wallet were born to satisfy this necessity, delegating the hurdle of the blockchain management to a central server. In this way, each light node asks the server only the pieces of data it needs to perform the required verifications on the transactions, so less hardware is needed, and wallets can exist also in the form of mobile applications. Of course, security is partially compromised, although many measures have been implemented to minimize the trust needed towards the full node providing the data (like changing dynamically the supporting full node, lowering the possibility of receiving malicious or fraudulent information).

Devices have been built to physically protect the key pairs. This *hardware wallets* are able to store such keys locally, embedding them on the individual item. Security is often ensured by the choice of a PIN code to unlock them and dispose payments, while in case of loss or theft a recovery code (usually saved offline in the form of a random set of words) can be used to restore the data and the funds on a new device. These devices combine great security standards with high portability and a relatively easy user interface. Examples are the Trezor wallet (see Figure 1.8) or the Nano Ledger.

Figure 1.8: a Trezor hardware wallet

Another primitive but highly secure way to store bitcoins are paper wallets: these are literally paper sheets with private keys printed on them. Usually the keys are not pasted in their binary or Base58 format, but properly encrypted (with a password one has to store elsewhere) or a QR code. They seem outdated, but actually printing a private key directly on paper is one of the safest ways to securely hold our funds, above all if the keys were generated offline: in this case the term we use is "cold wallet".

1.5 Transactions

Transactions are the basic constituents of the entire Bitcoin network. Everything else in Bitcoin is designed to ensure that transactions can be created, propagated, validated, and finally added to the global ledger of transactions, the blockchain (A. Antonopoulos, 2017).

A transaction is simply a data structure, which contains all the relevant information in order for all the peers to process the change in ownership of a given value of bitcoins.

The key elements of a transaction are:

- *Inputs:* what has to be spent in the transaction. Precisely, every movement of value takes some previous transactions that have not been spent yet (called UTXO, or Unspent Transaction Output) that adds to the desired amount.

- *Outputs:* the value that has to be sent with the related transaction. There's at least one output, the one of the recipient, even though most of the times past UTXOs don't sum up to the exact wanted number, so a change is needed.

- *Fee:* the fee is paid to the miner that will manage to include the transaction in the blockchain (explained in detail later), thus confirming it. Fees are not explicitly written in the data, but can be computed by every node, removing the sum of the outputs from the sum of the inputs.

- *Signatures:* these are the most important part of the transaction. In fact, while every other element (including unspent transactions of every account, which are public by definition in the Bitcoin network) can be easily written and aggregated in a candidate transaction by anyone, only the owner of the sender account can create the digital signature that makes the entire data structure valid. As we have anticipated earlier, talking about public key cryptography, the signature system of Bitcoin allows users to digitally sign the transactions they want to authorize, proving unequivocally that they have the rights to do that, but without revealing their private key.

This solution is incredibly elegant, because "it enables for the first time the exchange of value in a very secure way, over a highly insecure network" (A. Antonopoulos, 2017). Every node does not need to trust any other peer yet can be sure that the sender is authorized to spend the funds, if presenting the correct digital signature. In the credit cards networks, this would not be possible. Even though at the moment they're more at scale than Bitcoin, their network must be always kept secured, because sensitive financial information is transmitted in order to process the transactions.

Once signed, a transaction is propagated to the network, specifically to 7 to 10 peers at a time. Each node independently verifies it, checking that the sender has the private keys needed to spend the money. If the transaction is valid, the nodes propagate it to their peers, making it reach the entire network in some fractions of a second. If something in the structure is not valid, the transaction is not propagated, thus preventing attempts of spam or DDOS (Distributed Denial of Service) attacks.

As soon as the transaction is included in a miner's valid block and the block is correctly added to the blockchain the transaction is defined as confirmed and its output becomes a valid UTXO itself, that the recipient can spend whenever he wants. Essentially, the blockchain is a large database of all the transactions, made by every user of the Bitcoin network, since its birth in 2009. There are no balances written on them, but every node or wallet independently computes them.

1.6 Mining and Consensus

As previously stated, for a decentralized currency to exist, every participant must be able to independently validate all the transactions that the other nodes want to make (S. Nakamoto, 2008). In order to do that, everyone must therefore have a copy of the ledger which they can use to retrieve the balances of the transactions' senders and check if they have the rights to spend the desired amounts. Furthermore, the version of this ledger must be the same for all actors, otherwise conflictual validations would arise.

Every node must agree on a single and official history of the validated transactions, thus gaining and maintaining a *consensus:* this consensus on the transactions and balance history of the entire network (and all its participants) was the key element missing before Bitcoin, in order to create a pure decentralized currency.

In Bitcoin, it is obtained through a process called *mining*, which has two main objectives. The first is to increase the length of the blockchain (the number of validated transactions), keeping one single chain as the valid history for all the network's participants. The second purpose is to "create" and issue new bitcoins. In fact, new bitcoins are *mined* every time a block is created, guaranteeing to the overall network a stable and deflationary new money supply.

Figure 1.9 shows the projected issuance rate for the Bitcoin protocol:

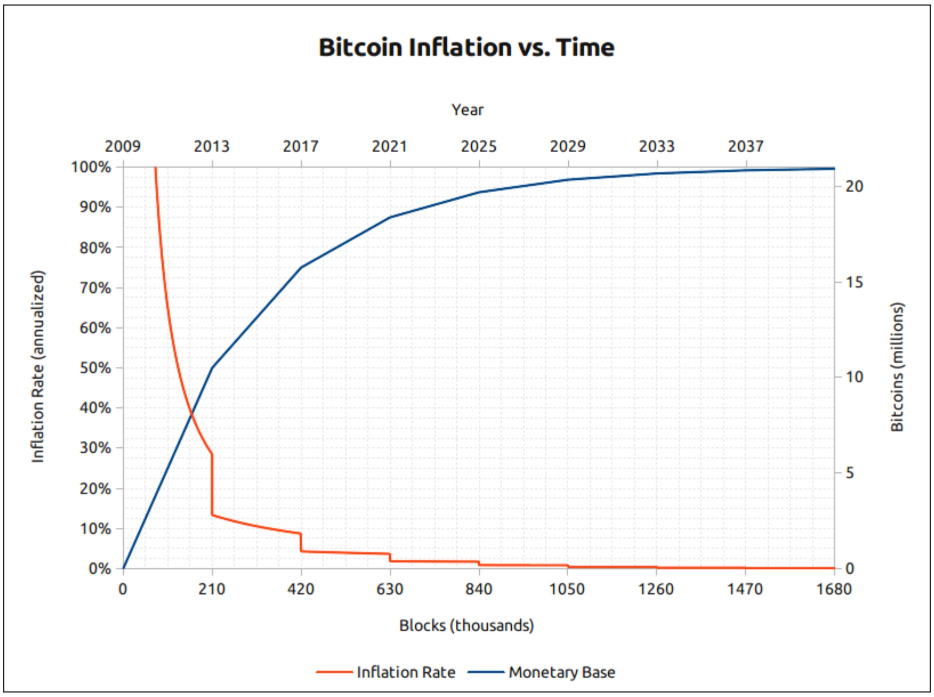


Figure 1.9: deflationary issuance curve of Bitcoin's supply through the mining process (Bitcointalk.org).

Miners collaborate on sustaining the network with their processing power, incentivized by the bitcoins they receive in exchange. In addition to the new bitcoins mined for every block, miners receive as a reward also all the fees of the transactions they include in their block.

Let's see the process of mining a new block in more depth, given that is similar for many blockchains and cryptocurrency projects and it is the centre of all blockchain security.

Participants compete on a simple and statistically predictable computational problem, based on a cryptographic hash algorithm. Since the problem is meant to be completely random, the probability of finding a valid solution is only proportional to the *hashing power* (or computational power) a node provides to the network. This mechanism is called *Proof of Work* because finding a valid solution implies that sufficient amount of work has been spent in the validation process. In this way, presenting a valid result is a proof of the work done for the network.

This invention has been the missing piece that all of Bitcoins' predecessors didn't have and prevented them from becoming the first true decentralized digital currency. Particularly, the invention mentioned in Nakamoto's paper makes possible to have an *emergent* consensus (S. Nakamoto, 2008). The word emergent means that is built and maintained over time, not in a fixed or scheduled moment (A. Antonopoulos, 2017).

As mentioned, participants compete on a simple and statistically predictable computational problem. In particular, they need to repeatedly hash a string of text until the resulting number (in hexadecimal format) is lower than the system's specified target. It can be visually seen as throwing 4 dices at a time, trying to obtain a number lower that 7 (Figure 1.10).

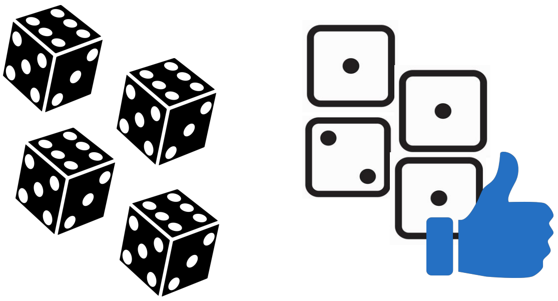


Figure 1.10: similarities between the mining process and a dice play.

With only some simple rules, coded in the Bitcoin protocol, every node is able to independently build a copy of the blockchain, knowing it is the most recent one and the one all the other nodes agree to use.

The entire process is made by four distinct activities, which are independently managed by the network's nodes:

- Every node independently verifies and implicitly authorizes every transaction
- Every mining node arbitrarily chooses a group of transactions, assembling them in what is called a *candidate block*
- Every miner constructs the block header, trying to obtain a valid proof of work
- Every node verifies the new block and adds it to the local copy of the blockchain

Let’s look at each activity more in depth:

Independent verification of transactions computed by every node: every node running the Bitcoin reference code will receive pending transactions from its peers and propagate them if valid. The validity of a transaction depends on a pre-determined set of criteria, which include:

- The data structure in which it has been constructed must be valid
- Has to contain at least one input or output
- The size doesn’t exceed the maximum allowed value (for bitcoin is currently 100 bytes)
- Every input the sender is willing to spend must exist in the blockchain and not have been already spent in other previous valid transactions
- The sum of the inputs must exceed (or at least be equal to, if no fees are planned) the sum of all the outputs
- For each input, a valid digital signature must be added. The digital signature is produced from the private key, without disclose it. Thanks to the irreversibility of the underlying cryptography, every node is able to check that the signature has been created by the correct private key, without seeing it

As previously seen, every note that validates a transaction propagates it to some of its peers (a number not so high, most of the times between 5 and 10 nodes). In this way, authorized transactions are seen from the entire network in some fractions of a second, while incorrect or fraudulent transactions are immediately stopped by every node deciding not to pass them on.

Aggregation of transaction into candidate blocks: after validating a transaction, every node will add it to a temporary storage called *memory pool*, where transactions not yet confirmed will remain until they're included in a valid block.

Some nodes of the Bitcoin network arbitrarily choose to run an additional part of the protocol, which gives them the right to participate in the collective "game" that takes place every 10 minutes for the creation of a new block. These nodes are called *miners*, and there are currently about 10'000 of them, at the time of this writing (Bitnodes.earn.com, 2018).

When mining nodes receive a transaction, which is declared valid, they proceed in adding that same transaction to their current *candidate block*. A candidate block is properly structured but cannot be confirmed and added to the blockchain until a valid proof of work is provided from the miner, which is found as a solution to the Proof of Work algorithm.

A block has a size limit, currently 2 Mb (En.bitcoin.it, 2018), therefore a miner must choose which transactions have the highest priority. The criteria for this choice are:

- The age of the transaction UTXOs, that is calculated based on the date of the block in which they were confirmed. Older transactions have higher priority
- The value of the inputs, so transactions that move more value tend to be processed earlier
- The amount of fees that the miner will earn if the transaction is included in the block he manages to validate. Let's remember that fees are arbitrarily chosen from the sender (or the sender's wallet) in an implicit manner, as difference between the total inputs and the total outputs

The first transactions a miner will include in his candidate block is a special type of transaction, called the *coinbase transaction*. It doesn't spend any previous output and contains only one input, called the coinbase. The output consists of the value of the current mining reward and has to be paid to the miner's personal bitcoin address; the coinbase transaction is responsible for the minting of newly created bitcoins mentioned earlier.

The rewards for the newly created blocks depend on the current block height (the length of the blockchain). This rate started as 50 bitcoins for every block in 2009, when the Bitcoin network was born, and has halved every 210'000 blocks (approximately every 4 years). This mechanism, called *halving*, will cause the issuance of all 21'000'000 existing bitcoins in the year 2140, if the block creation rate remains constant.

Just as the other transactions, also the coinbase transaction has a data field, which can be filled by the transaction's creator with arbitrary information. As a side note, the first block mined by the personal computer of Satoshi contained in the coinbase data field the following string of text: "The Times03/Jan/2009 Chancellor on brink of second bailout for banks", with a double function. First, it acted as a proof of timing for the birth of his protocol, and moreover served as a reminder for the reason this invention was needed so much and so fast.

Construction of the block header: the block header can be seen as the title of every block and it's the key for the entire blockchain structure. It is composed by six fields:

- A Version number (4 bytes) use to specify the protocol version and to track the latest updates
- A reference to the previous block hash (32 bytes). The fact that every block must contain in the header the hash of the previous one is what links every block to its predecessor and successor, forming a chain whose integrity and immutability is strengthened as the blockchain itself grows
- A Merkle Root hash (32 bytes): it is a hash of the root of the Merkle Tree of all the transactions included in the block. In other words, it can be defined as a "fingertip" of the combination of all the transactions, and it's important because any change of the underline transaction database

would make the root change and, as a consequence, the solution to the proof of work would change too. Changing an older transaction would cause the block header to change, and this means the following bocks must be re-created, because they have to be linked to the new block header

- A Timestamp (4 bytes), which is represented in seconds from Unix Epoch (January 1st, 1970) and declares the approximate creation date of the block
- A Difficulty Target (4 bytes) which represent the threshold, under which the proof of work must fall, in order to be considered valid
- The Nonce (4 bytes): a completely arbitrary data field that the miner can fill with whatever number he wants. This is the field that all the mining algorithms change, hoping that the hash of the total block header will result in a value under the stated difficulty. At the time of writing, approximately $1{,}8 * 10^{21}$ random nonces are needed in order for the entire network to find a suitable one in about 10 minutes

Then, every miner starts trying different values of the nonce until the block header hash (obtained with the SHA-256 algorithm) is less than the current difficulty target.

Addition to the longest current blockchain: when someone finds a valid solution, the candidate block is propagated through the Network, until everyone agrees on a unique version of the new blockchain. As miners receive a new valid block, they will interrupt the current "match", create a candidate with the reference to the new block, and repeat the process from the beginning, in a continuing cycle that has sustained the Bitcoin ecosystem since January 2009.

It can happen that two or more miners will simultaneously find a valid block (resulting from two valid solutions of the proof of work algorithm). In this case, all the other miners will start to work on the block that reached them first. So, until a new valid block is mined, two blockchains will compete for being the longest (and, as a consequence, the valid) one: this phenomenon is called *fork*.

Forks of this type happen quite often and are easily resolved after about ten minutes, when the new block is created and will make one of the two blockchains the longer. But there are other situations, in which blockchains are divided on purpose: these are called *soft forks* and *hard forks*.

Soft forks happen when the network, in the form of its miners, agrees on an increase of the validation rules of the new blocks, for example when a new protocol update adds more capabilities to the blocks or transactions data structures. In this way, what happens in the original blockchain is still valid in the new one, which only admits more functionalities.

On the other hand, when a hard fork happens, the network splits in two separate chains, essentially restricting the rules for consensus and block validation. For example, when on August 1st, 2017 the Bitcoin hard fork took place, the new blockchain that was born became a completely new cryptocurrency (called Bitcoin Cash), with a new set of rules that were different from the ones of the original Bitcoin Core implementation, that remained valid.

1.7 Mining concerns

The costs of the mining activity can become quite significative and are steadily growing to a higher and higher rate. For the first years, it was possible to mine some blocks also with a personal computer, as the earliest adopters did. But the more Bitcoin gained popularity, the more difficult it became to find a suitable solution for the proof of work algorithm: the software is programmed to dynamically change the difficulty target, in order to maintain a block rate of one every ten minutes.

Every 2016 blocks, the protocol calculates the rate and retargets the difficulty, so during the years miners started to use more sophisticated hardware to achieve their objective. CPU have been abandoned and GPU used instead, which were more efficient and powerful. Then, ASICs (Application Specific Integrated Circuits) were invented, which are electronic circuits built specifically for Bitcoin mining, able to achieve incredibly higher levels of efficiency than normal graphic boards.

This technological advancements in mining hardware, combined with the entrance of so much hashing power (computational effort of the new miners) has two main hurdles: first, it significantly centralizes the network, which was meant to be completely decentralized. With the appearance of mining pools, which are organizations of miners that share their hardware in exchange of a fraction of the reward if someone of the pool finds the new block, the network now is dominated by a handful of players, mostly located in countries with low energy costs (see Figure 1.11).

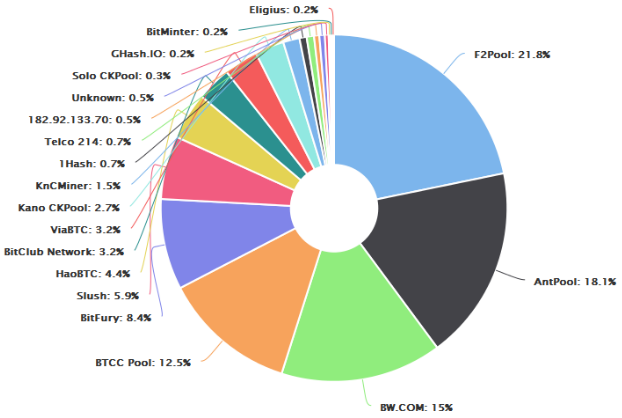


Figure 1.11: main Bitcoin's miners and mining pools (cnbc.com).

Decentralization is critical for the security of the network, given that potentially anyone with more than the 51% of the hashing power could try to impose his malicious version of the blockchain with a significant chance of succeeding.

The energy costs related to the hardware are growing as well, reaching 71 TWh per year at the time of this writing (Digiconomist, 2018).

Solutions are already in the testing phase. The most notable one is called *Proof of Stake*. Essentially, instead of receiving a reward based on the computational power one provides to the network, in this new paradigm miners get compensated proportionally to the amount of actual coins they put as "collateral". The more coins one invests (which are not spent but blocked as collateral and lost in the case of a malicious attack attempt) the more probability he has to mine the new block.

This hardware-free consensus protocol is currently in beta testing for the world's second cryptocurrency, Ethereum, but many other implementations have been proposed.

1.8 Other Blockchains

Even if, as stated in the chapter introduction, Bitcoin is the first cryptocurrency and the first working example of a blockchain, it is certainly not the last and for some applications the most influential. Given that the original reference code of the protocol was open source, everyone interested in creating their bitcoin-like alternative currency could easily fork it (make a copy and modify it as he wanted).

Therefore, since 2010 many other projects were born, with purposes ranging from improvement of Bitcoin technology to pure speculation.

Coloured coins were one of the first examples: the original Bitcoin code was maintained, but the creators added a feature that made possible to attach a "digital label" to little amounts of bitcoins, converting it in another asset of any form. You could "colour" 1$ of value in BTC with a certificate representing ownership of a company's share, and exchange that same chunk of bitcoins as if it were exactly that stock.

Another alternative coin, or alt-coin, derived from the Bitcoin protocol, is *Litecoin*, which is today the sixth biggest coin, with a total market capitalization of about 5,6$ Billions. The founders made two important changes: first, they chose a different Proof of Work algorithm called *Scrypt*, which was built to be ASIC resistant, thus preventing the centralization phenomenon seen before for Bitcoin. Second, they shortened the average block throughput rate to 2,5 minutes. These features make Litecoin, to its followers, more suited for retail purchases and frequent uses.

The most notable alternative coin (at this moment the second biggest cryptocurrency after Bitcoin) is Ethereum. Born in 2015, Ethereum's purpose is far from being only a digital and exchangeable asset: the coin "ether" is meant to power what is called the Ethereum Virtual Machine (EVM), a sort of global and distributed computer in which everyone can run code (called *smart contracts*) which benefits of all the advantage blockchains bring, such as immutability, transparency and security (Buterin, 2014). The main difference is in the scripting language: while Bitcoin's language is intentionally limited for security reasons, Ethereum's one is "Touring-complete". This means that all sorts of code structures can be created. Security is maintained in the EVM through a fee system, in which users pay for contract execution that is computed by a miners' network similar to the Bitcoin's one. A program is triggered with a payment of any value, plus some data that act as inputs for the execution. The sender decides (or the wallet sets in an implicit fashion) two key variables:

- *Gas Price*: the cost per computational step (paid in ether) he is willing to pay. Computational steps are precise fractions of the contract execution, whose amount is known in advance since the code is open source
- *Gas Limit*: the maximum number of computational steps allowed by the sender

Multiplying these two values one gets the highest amount he can pay for the contract use. When sending the initial transaction, the protocol immediately withdraws this total amount as a safety deposit from the sender's account. After the complete execution of the contract, what remains of the safety deposit is sent back to the original account. If the maximum fee is reached, all of the safety deposit is lost, and the contract completely reverted: that means all the computation it has already concluded are cancelled.

1.9 Public and private blockchains

An important definition, used to classify existing blockchain solutions, is between public and private ones. Both solutions can have the same protocol features, such as consensus algorithm, immutability and decentralization (to different degrees). What differentiates them is the possibility of nodes to enter the network.

In a *public blockchain*, nodes can freely enter the network, without any limitation. This is the case of the most notable blockchains, like Bitcoin's or Ethereum's. Nodes are incentivized through a system of fees and rewards and can leave and join the network at any time if they want.

On the other side, in a *private blockchain* only some specific actors are allowed to act as nodes. The company multichain, for example, enables its clients to create every type of private blockchain the need, varying the constituent parameters and granting the necessary authorization to the selected peers (Greenspan, 2015).

Although a private blockchain seem counterintuitive, in a world where decentralization and distributed power are the main purposes, some notable solutions have been built. This structure, in fact, enables the creation of a hybrid network where some actors, who normally use an intermediary to manage the relationships, can reach and maintain a consensus on a continuing basis, without taking the risk of being fully transparent with the outer market.

The concept of public and private ledgers can be further dissected. While the mentioned dichotomy depends on the right that nodes have in participating in the network from a user perspective (transmitting transactions), there's also another distinction that has to be made, which is between permissioned and permissionless blockchains.

In a *permissioned* network, only some selected nodes can manage the protocol and approve changes to it, while in a *permissionless* blockchain (like Bitcoin's) every node is able to suggest a protocol update and fork its variant.
This double distinction creates a series of 3 major classes of commercial blockchains, which we'll briefly cover below:

- *Permissionless Public Ledger*: such a protocol is inherently accessible by everyone. No limitations are imposed to nodes that want to access the network or leave it. Furthermore, miners and validators are unknown and untrusted. The most notable example is the Bitcoin blockchain.

- *Permissioned Public Ledger*: in these systems a limited number of validators are admitted (which can be also democratically chosen from the user base), but there are no limitations for the users' admittance. Some examples are Ripple and Neo.

- *Permissioned Private Ledger*: there is a selection both to participate and to vote and act as a validator of the network. Such blockchains are normally built for business consortia or aggregates, when sensitive information is shared between the peers. Technically these structures lose most of the decentralization that public ledgers provide, but costs for transactions and latencies can be dramatically reduced

Its straightforward that a permissionless private blockchain can't exist, because of the opposition of the two concepts.

Chapter 2 – Blockchain as an Innovation in the Field of Logistics

2.1 Introduction

The innovation a new technology brings is not always enough for it to reach meaningful scale. Drivers for innovation are mandatory: in simple terms, there must be a need or a desired improvement that the technology can satisfy, otherwise the resistance to change will prevail.

In the following paragraph the main drivers of the logistics sector will be examined, detailing the benefits blockchain technology could bring. These are the high presence of *manual and paper-based processes*, the *interdependence of different process flows*, the increasing *desire for greater transparency* along the chain, and the significant losses caused by *counterfeiting*.

2.1.1 Paperwork and manual processes

Even though new technologies are slowly revolutionizing every aspect of the supply chain, the logistic industry remains full of manual and paperwork-based processes: It has been estimated that between 15% and 50% of the costs of the transport can be allocated in the management of the trade-related paperwork (Groenfeldt, 2017). Moreover, for heavily regulated processes like customs clearance procedures, manual data-entry and paper documents are still highly in use.

This of course increases the risks associated with the process, particularly in terms of:

- *Risk of counterfeit*: paper is much easier to alter at our own advantage, in fact documents like the Bill of Lading are often subjected to fraud. A digitization of the shipments' relevant documents, even without any blockchain implementation or any trust minimization technology, would significantly decrease the rate of frauds happening in the logistic sector.

- *Human error*: needless to say, although computers and IT systems are not 100% reliable, manual procedures have a higher probability of containing inaccurate or incorrect information: it is estimated that a stunning 10% of all freight invoices contains inaccurate data, which leads to disputes and all sorts of process inefficiencies along the supply chain. With thousands of different transactions happening on a daily basis, reconciliation of discrepancies is a costly and laborious activity which profoundly impacts every stakeholder involved. Furthermore, at least 5% of the total freight spend could be saved through improved invoice accuracy and reduction of overpayments (DHL Trend Research, 2018).

- *Planning & forecasting constraints*: Information about freight movements goes through the supply chain with a delay (Credits' blog, 2018). This effect, added to the necessary reconciliations that have to be made between different databases involved, makes forecasting a difficult task for the stakeholders, which most of the times must do their planning analysis on relatively scarce and not updated data.

2.1.2 Physical, information and financial flow

A typical logistics supply chain is made of three different flows (Comelli, 2008). The first is the physical flow, responsible for the purchase, transformation, manipulation and delivery of the products.

The second is the information flow, that tends to be coordinated with the physical one, and involves the creation and transmission of relevant cargo documentation, customs declarations and certificates, and back-office paperwork. However, documents delays are common and can cause in many cases significant delays in cargo movement, as well as demurrages costs in case of permanence in port.

Finally, a financial flow is responsible of guaranteeing the correct timing of monetary transactions; normally the financial and physical flows of some goods are not synchronized, and most of the times financial operations are only locally optimized (Comelli, 2008), like between a supplier and its own trade finance partner.

The flows integration is usually made by enterprise information systems based on software tools like Enterprise Resource Planning (ERP) and/or Advanced Planning and Scheduling (APS) (Comelli, 2008). However, these centralized systems all share the disadvantages of having information stored in separated data silos, like reconciliation costs and higher risk of counterfeiting and human error.

2.1.3 Need for transparency

The demand for greater transparency in modern supply chains is increasing. Knowing exactly the history of a product is becoming mandatory; on the first hand because consumers start to care more and more about the conditions and want to be sure companies acted coherently with their social responsibility standards. Secondly, big organizations and consumer-facing brands are raising the bar of openness about their processes, in order to gain the clients' trust, thus fueling this transparency wave into the entire space.

Frank Yiannas, Walmart's vice president of food safety, conducted an interesting experiment in late 2016. On his way to work, he went to a Walmart store, bought some sliced mangoes and put it on the table as he arrived in the office, asking to his team: "Find out where these mangoes came from, I set the timer". It took almost 7 days to give him back an answer.

Yiannas later decided to run a pilot test in collaboration with IBM's blockchain division, in order to have greater and up to date visibility on the product state in every moment. In the project, mangoes shipments were tracked and digitally registered on blockchain with numeric identifiers from the moment the farmer harvested them; 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.

When, some months later, Yiannas repeated the experiment, the result was significantly changed. He just prompted a code printed on the label on a web portal, and in a few seconds the following information appeared: 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.

2.1.4 Counterfeiting

Fraud costs the global economy more than $600 billion a year (Research.ibm.com, 2018). Reports show that counterfeit and pirated products are being produced and consumed in virtually all economies, with Asia emerging as the single largest producing region (Zeliha, 2014). Particularly complex supply chains, made of multiple suppliers in different geographical areas, make it hard to prevent malevolent actors from tampering with everything, from paper currency to consumer electronics. These products known as counterfeits are identical in appearance to the authentic brand and fraudulently display the brand name being copied (Cohen, 2005).

In the past, counterfeiting activities were limited to high-priced exclusive merchandise. However, the increased activities in international marketing and advancements in technology have allowed counterfeits to penetrate into lower priced intensively distributed, non-durable goods (Byrne, 2007). According to recent estimates, New York City alone lost approximately $350 million and 25000 jobs a year due to the counterfeit market (Geiger-Oneto, 2007).

Counterfeit products result in consumers paying higher prices for legitimate goods, as companies are forced to pay additional costs associated with improved packaging and the efforts used against counterfeiters. Furthermore, the sale of counterfeit goods creates an unfair competition that drives down sales of the rightsholders, possibly resulting also in job losses.

The items that counterfeiters and pirates produce and distribute are often substandard and can even be dangerous, posing health and safety risks that range from mild to life-threatening (Zeliha, 2014).

2.2 Types of solutions

The logistic and transportation market is currently affected by a superficial and insecure understanding about the possible uses of the technology. Moreover, the literature does not provide any categorization of the potential uses of blockchain in logistics. The aim of this paragraph is to isolate and briefly describe the four main clusters which efforts have been invested towards. Many problems will be probably not mentioned, giving priority to the most urgent matters, the ones that could result in the biggest advancements if solved.

These topics are the *digitization of cargo documentation*, especially the Bill of Lading, the *optimization of the trade finance* flows, the *product traceability and anti-counterfeiting* and the *IoT automation and smart contract integration* into physical objects.

Let’s deep dive into each one of them.

2.2.1 Bill of Lading & cargo documentation digitization

As we’ve covered before, the transportation of some goods involves not only the physical movement of the freight, but also the transmission of all the related cargo and customs documentation, which include Bill of Lading, Manifest, Notification of dangerous goods, Discharge List, and so on. This information flow is acknowledged to be equally important as the physical flow since it enables stakeholders to efficiently perform their tasks (Pruksasri et al., 2014).

However, despite the growing digitization, most of these documentations still travel in paper copies (Takahashi, 2016; Pruksasri et al., 2016). Furthermore, in case of mismatch between the information on the documentation hard-copy and the reality, the issue is solved with bilateral means of communications (Phone calls, emails), which are not efficient in a network perspective.

This forces every company to create its own cargo information and redundantly align with the network in order to ensure its correctness during the process, which causes lead time to increase and costs to soar as well. Many data are also kept secret in companies' data silos, posing a centralization risk in case of loss or cyber-attack.

The feature of blockchain that raised the interest for this type of applications is its capacity of creating unique digital assets, which cannot be duplicated nor deleted, but only transmitted in a secure and transparent way. This warranty enables the creation of a unique documentation that does not change throughout its life-cycle, so that the holder of the document can exercise the right to claim the performance of the obligation (Takahashi, 2016).

Many attempts to digitize the Bill of Lading have been made in the past. Since 1986, some experiments of digital registries have emerged, but they were always closed or with members selection, never reaching critical mass of adoption (Takahashi ,2016).

As we've seen, cargo documentation is usually transmitted (digitally or manually) from one actor to another, in a direct and often redundant way. Peers follow some specified rules for sending the documentation in a specified way, respecting some hard deadlines. This logic can be seen as a *push* one, where the data movement is generated by the instruction each actor has been given from the network leader or the common set of procedures. What blockchain aims to realize is a common database, a *ledger*, where each information creator can upload its documentation, while the other participants are able to retrieve the data if and when they're needed. This, on the other side, can be seen as a *pull* logic, in which information is safely stored on a common blockchain and is available for everyone, who can retrieve it at any time. A graphical explanation of the flow can be seen in Figure 2.1 below.

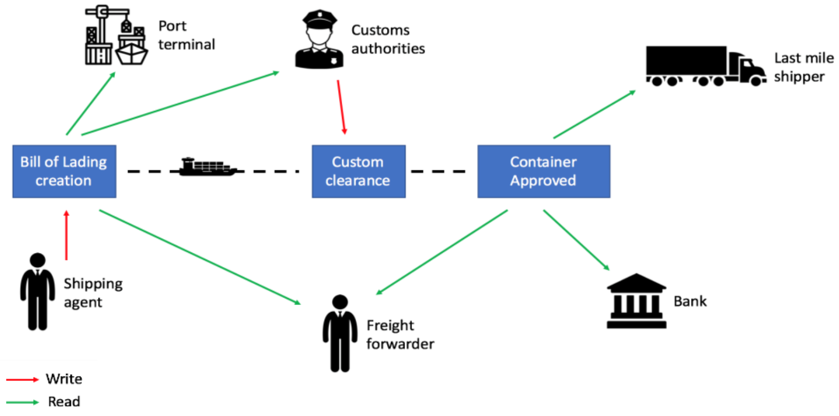


Figure 2.1: Blockchain implementation for cargo documentation digitization.

Information owners can be the freight forwarder, the shipping agent, the port logistics operators and so on. By cryptographically signing their data, the entire network can verify that they were responsible for uploading and/or updating the information under their competence area.

Following modification or omission of data can be easily detected, thanks to immediate access to the history of the documentation, reducing fraud attempts or errors by a huge factor.

These types of blockchain implementations mainly focus on digitizing and validating the Bill of Lading, one of the most important documents in international transportations. Companies like Blockfreight, Skuchain or CargoX have clearly stated this as their main purpose, given the possible savings and lead time improvement such a revolution could bring.

2.2.2 Trade finance optimization

Trade financing is known to be characterized by large inefficiencies and high chances of frauds (Skinner, 2016). For instance, the U.S. market accounted for losses that reached 0.5 billion US dollars in 1995 due to trade finance frauds (Barnes and Byrne, 1996). Similarly, the Commercial Crime Bureau recorded a loss of 2.4 billion Hong Kong dollars (around 0.3 billion US dollars) in 1998 (Zhang, 2011).

One of the most common counterfeits involves the letter of credits, that are used for financing international trade operations. For instance, fraudulent actors can falsify the documentation needed to receive payments from the bank, even when products are inexistent, or of minor than specified quality. Today, banks protect themselves from this type of frauds by asking for additional confirmations and certificates. All these activities naturally drive up costs and increase operative lead times, given that in many cases financial payments are the bottle-neck to the entire flow. For example, containers are usually hold in the terminal until they do not receive the proof of commercial viability from the financing bank.

One of the reasons of these reconciliation delays is that banks and financial institutions are usually not included in the operation procedures but are only notified when an action from them is needed. The use of a blockchain, towards which every actor poses absolute trust, could enable the inclusion of trade finance intermediaries in the ledger, where they would be able to monitor in real time the advancement of the transportation and port operations. This would speed up dramatically the waiting time needed for a payment to be processed, improving the operative lead time as a consequence.

At least some types of payments and funding could be also automated, thanks to the use of smart contracts as escrow accounts. Money can be cryptographically blocked in a specified account and freed only when and if certain conditions from the debtor are met. The openness of blockchain technology could ensure that the contract terms are respected, even without disclosing the identities of the involved parties and the value that is exchanged.

2.2.3 Product traceability and anti-counterfeiting

Moving a single container or product involves an incredible number of actors over an international, inter-company and inter-cultural network in most cases. Every step of the process increases the possibility of losing information over the freight, due to human error or malevolent theft attempts; On the other side, companies pretend more and more visibility over a product history, aspiring for real-time data updates.

The lack of visibility is often a consequence of the fact that information is held in multiple data silos and accessibility for the different actors is limited and/or fragmented. As a consequence, continuous alignment is necessary, and process lead times increase, while visibility doesn't seem to improve.

By taking advantage of the timestamping functionality of both public and private blockchains, companies can use one single source of truth to store and update the information on a manipulated container or product. Every time a significant operation is made on the freight, such as change of ownership, loading or unloading of LCL cargo or customs operations, its status is updated on the blockchain, digitally signed by its current owner and paired with an immutable timestamp that certifies the time of completion of that action. A cryptographically secure history of the product can be created and used as proof of authenticity against counterfeit or government controls. Other network participants can then monitor these operations in real time as they're uploaded.

Below a scheme of the interested flow (Figure 2.2):

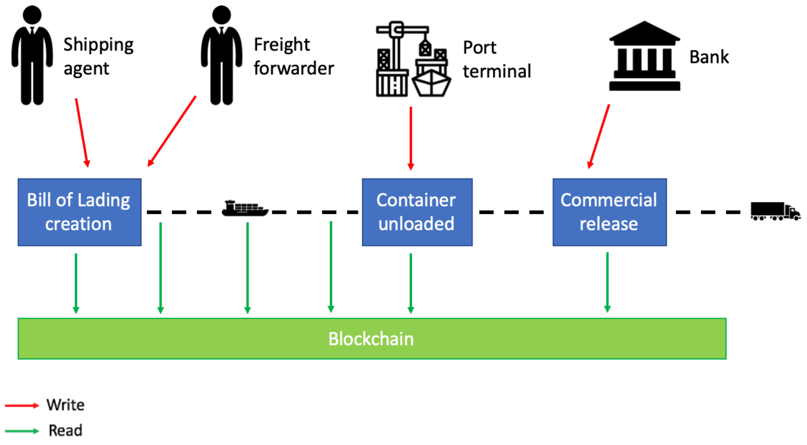


Figure 2.2: Blockchain implementation for product traceability.

As we see from the picture, blockchain would act as a single source of truth for all the actors, that can independently retrieve and verify the complete product history in a quasi-real time fashion (depending on the sensors infrastructure used). Some participants have the right to upload the status of the goods, like port terminal in case of a container successfully unloaded from a vessel. Other peers are notified of these changes or can freely access the same information: the financial partner, for example, could be able to see the confirmation of the container unloaded, because that triggers its payments to the respective parties.

2.2.4 IoT & smart contract automation

Blockchain can assure its users that the data has not been modified or deleted over time, guaranteeing an immutable source of reliable information. However, the authenticity of the data that is uploaded on the ledger in the first place still depends on the users. Many believe that IoT can be a possible solution for this problem.

IoT mainly consists of embedding sensing and communication capabilities to a wide range of physical objects and connecting these devices to each other over the internet so that they can monitor their environment, communicate their status, and even take actions based on the information they receive.

The combination of IoT and smart contracts could lead to process automation, regarding all the interested flows: material, information and financial ones. Sensors with integrated GPS technology could be embedded in the container, registering its position on the blockchain for all the authorized actors to see. Furthermore, humidity or temperature sensors could monitor the goods conditions, which is critical when food or pharmaceutical freight are transported.

In order to be able to update some data on the blockchain, sensors must possess and manage a key pair, that can be electronically embedded in the hardware, in the same way as we've seen before talking about hardware wallets like the Ledger or Trezor. In this way every chip could be easily recognized because it would be tied to a public key on the blockchain that is unique, thus making counterfeit of the position or physical condition of the container extremely difficult for an attacker.

Having such updated and trustful data at disposal makes many automations possible when combined with smart contracts that can be triggered by the same sensors. Low value-added operations like loading or delivery confirmations can be automated, but also more critical steps like the issuance of financial payments from the bank when the container is successfully unloaded.

Furthermore, customs import operators could have a precise history of the conditions of the goods during the entire voyage, including if anyone ever opened the container and if the mass has changed. Having this knowledge in advance, customs clearance procedures become faster and more effective.

The problem of giving a unique digital identity to a physical object is currently studied by many actors, as we'll see later. IBM is one of the research leaders, developing what they call "crypto anchors": they consist of tamper-proof digital fingerprints that can be embedded into products and linked to the blockchain (Research.ibm.com, 2018). They can take many forms, from miniaturized computers to optical or genetic codes, like the one shown in Figure 2.3.

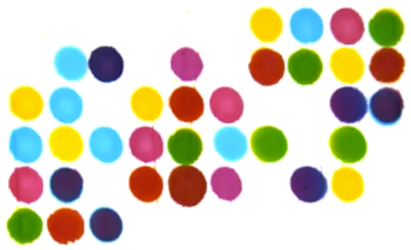


Figure 2.3: Example of an optical crypto anchor (IBM website).

In the picture we see an example of optical crypto anchor, printed on the product with a magnetic unremovable ink. The consumer just needs to scan it with a camera and look for the same code in the ledger of the allowed ones, confirming that is valid. Crypto-anchors are highly secure because they are embedded in the product and consist of cryptographic mechanisms that provide unclonable identification.

2.3 Blockchain threads

We've seen that blockchain's potential can go well beyond any purely financial and monetary application, especially in the field of supply chain management. This technology could promote a complete paradigm shift, putting openness and transparency ahead and saving enormous capitals currently trapped in intermediaries and useless and redundant re-conciliation systems.

On the other hand, it's clear that distributed ledger technology is still in its infancy, and therefore has many technological challenges to overcome in order to reach full scale. The problems we'll list in the following paragraph are posing a threat on blockchain's credibility and represent the most urgent tasks for any researcher or developer working in the space.

As we've described in the previous chapter, Bitcoin's blockchain has some important technological limitations that currently undermine its scalability. These problems are common to all the public blockchains and are one of the primary obstacles to a broad usage of the technology.

2.3.1 Throughput rate

The rate at which blocks are validated is fixed in every major blockchain. Given that usually blocks have also a maximum dimension, it easy to compute a parameter that we call *throughput*, that represents the number of transactions a blockchain can process in a given timeframe.

For Bitcoin this number is extremely low, about 7 transactions per second (or *tps*). A common centralized network like Visa or Mastercard is capable of processing more that 10'000 transactions per second, so about 3 orders of magnitude above. For newer blockchains like Ethereum this number slightly increases (at about 50 tps) but it's obviously not enough for covering the broad range of supply chain applications that developers aspire to build.

However, solutions are currently tested, mainly related to *off-chain payments channels*. In simple terms, this range of solutions proposes the creation of private payment channels between two or more nodes, in which transactions happen virtually without any cost or latency. The reason is that they happen and are initially settled off-chain, meaning none of them has to spend the fee and wait the confirmation time of being included in a block. When the payment channel is closed, all the transactions are settled on the main blockchain at once, minimizing the associated costs. Security is guaranteed by requesting a collateral sum of money to be locked before opening the channel: this sum will be lost if the node is acting somehow maliciously.

2.3.2 Latency

This is a direct consequence of a low throughput. As we saw in the previous chapter, every transaction takes some time to be confirmed, and thus to be securely spent from the original receiver. This time varies, depending on the considered ledger: in Bitcoin a transaction may take up to one hour to be considered irreversible, whether in Ethereum some minutes may be sufficient. While these timeframes are acceptable for some use cases, retail and micro payments applications become impracticable.

The aforementioned payment's channels could resolve also this issue, in addition to a collaborative regulation work aimed to calculate the minimum acceptable time for a blockchain transaction to be considered legally valid and confirmed.

2.3.3 Centralization Risk

Blockchain removes the need for a trusted intermediary or ant certification institution, allowing the participants to fully trust the system and the technology behind it. This frees from many limitations of the past process structures but poses a significant risk in case distributed systems retain some type of centralization, because no controllers could intervene.

2.3.4 Transactions costs

Fees are an intrinsic element of all public blockchains, and they're normally required in exchange for the security and decentralization they provide. They act as an incentive for the nodes that carry the computational heaviness of the entire network.

Moreover, fees are not usually fixed: in both Ethereum and Bitcoin, the amount that has to be paid to the miners varies, on a marketplace basis. In particular moments, when the network is near saturation, higher fees may be required if we want our transactions to be confirmed soon. Added to the aforementioned throughput rate limitation, this fact implicates that public blockchains are an expensive infrastructure, compared to the existing centralized systems.

The graph below (Figure 2.4) shows the historical fee value, in USD, since the Ethereum *mainnet* was born. We can see that the average price is around 0,5$ recently, but in some periods this number can become much higher, as in January, 2018 when it reached its maximum value around 4$.

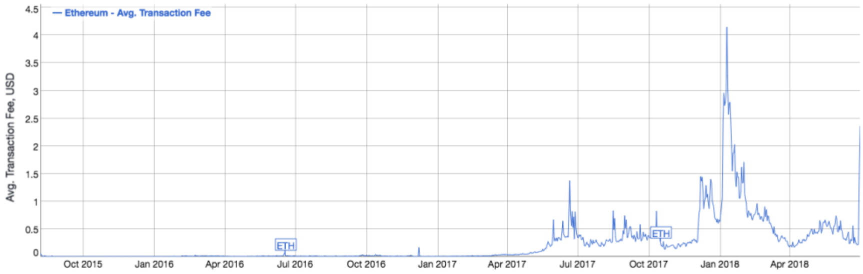


Figure 2.4: Ethereum fee daily average price since 2015 (www.bitcoinofamerica.org).

Imagine creating a project that uses the Ethereum blockchain as its backbone for decentralization. By definition, every time you want to change the "state" of your variables, you must submit a transaction, paying the related fee. It naturally becomes even harder when the price for that transactions is not fixed, but instead changes unpredictably over time.

Naturally, many solutions have been proposed and tested by developers and industries. The fees have to be paid in order to register a piece of data on the main blockchains, but it's possible to create what is called a *sidechain*. It consists in a separate blockchain, usually created taking a main blockchain as reference and changing some parameters of it, in order to make it more suitable for the desired application. Sidechains are completely disconnected from main chains, posing no risk on them and at the same time minimizing their inefficiencies, like tps or confirmation fees.

For example, if someone thinks the Ethereum blockchain is too expensive for its case study, he could fork the original chain and modify its code in order to minimize or delete all the fees involved (probably lowering the overall security of the system, so trade-offs have to be made). These sidechains can be then linked to the main chain through some predetermined transactions, usually performed to settle the current state on the more secure blockchain.

2.3.5 Inaccessibility for average users

As the reader can comprehend in the previous chapter, the technology behind a working blockchain or distributed ledger is quite complicated for the common user of the web and information systems we have nowadays. Even for using and safely storing a private key, some basic security principles are required to the customer, who is used to a simple login/password system where credentials can be easily restored in case of loss.

By giving the final user so much responsibility and freedom over his funds, cryptocurrencies reduce the number of reachable audiences only to the most expert and interested ones. Naturally there are some user-friendlier solutions, like exchange websites, hardware wallets and mobile applications, but usability remains one of the core obstacles to broad technology diffusion.

2.3.6 Lack of standards

Blockchain, like every new technology in its infancy, lacks a common or some common standards. As we've covered, many different projects exist, and many are created every year with the aim to solve the known issues from many different angles. Therefore, all 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.

Some experts state that there will be no single standard for blockchain applications and implementations, especially in the supply chain and logistics field, but instead "there will likely be multiple private permissioned blockchains due to the competitive nature of the business" (DHL Trend Research, 2018).

The creation of large consortia and community project specifically focused on this problem (like the Hyperledger project) is a great sign of a shared interest in better understanding and directing the research to a more useful common ground for innovation.

2.3.7 Industry adoption

This is certainly one of the most important challenges facing business adoption of blockchain technology. The distributed nature of this innovation enhances the "social" aspects of it: the more actors join this paradigm shift, the more benefit there will be for new entrants. In fact, similarly to the most common social networks "the value of the community increases when it is adopted by a growing number of relevant stakeholders" (DHL Trend Research, 2018). A critical mass is needed however, to put this mechanism in motion.

The first actors encountering this technology will ask themselves why they should increase the openness of their supply chain networks, seeing more disadvantages that advantages in the process. The more companies and institutions achieve the new approach, the more convenient will seem for new peers to join. At some point it could become an indirect (or direct) requirement, because consumers and industry leaders will get used to such transparency, thus raising the bar for surviving in the market.

2.3.8 Public opinion

Cryptocurrencies have been heavily criticized by the public opinion since their birth, because of their illicit uses in money laundering and drug related activities. Although it is important to state that Bitcoin and Blockchain are two linked but different concepts, it’s natural that these concerns have been also associated with blockchain technology in the last year, sometimes fostering a perceived distrust on the entire ecosystem.

One of the first and most memorable events was the Silk road website: a web marketplace positioned in the “dark-web”, in which people could exchange bitcoins for illegal substances and services. The security of the Bitcoin protocol guaranteed the anonymity of the sellers and the buyers, making the site reach incredible traffic during 2013, before its founder was arrested by the FBI.

Many other examples of Bitcoin (and cryptocurrencies in general) uses for illegal activities are still present today, like the CryptoLocker hackers that recently became famous in Italy for sending a virus via email to their targets, blocking all their relevant files. The files could be retrieved only with a password they would provide in exchange for a fee, paid in bitcoins.

Although the anonymity of the coin appears to help such actors remain secret, it’s worth remembering that blockchain technology itself can provide the opposite effect. All the transactions ever happened on the network are permanently saved on the ledger and can be seen from everyone. Thus, even if one address is somehow leaked (which in specific situations can be performed easily from the police forces), all its transaction history can be retrieved in seconds.

There have been other scandals, that have contributed to undermine cryptocurrencies’ (mostly Bitcoin’s) reputation, mainly related to the financial sector. The most notable is the Mt-Gox scandal of 2014 (Biagio, 2018): it was the most used exchange of that time, a site where you could exchange fiat money for Bitcoins. The site proposed a hybrid solution for the currency use: while communicating directly with the Bitcoin Blockchain for deposits and withdrawals, it didn’t provide the users their key pair for accessing the funds and used instead a classic login system as a security model.

During 2014 the site got hacked, and more than $300 million dollars in value were lost (roughly 13% of the total market cap at that time), generating a significant drop in the price and a loss of trust in the entire system (Biagio, 2018). Here too is worth underlying that the Bitcoin protocol wasn't hacked, but instead what got leaked were the private keys of the users, stored on the website central server.

2.3.9 Regulation

Cryptocurrencies, especially Bitcoin, were born from the anarchical willingness to exchange and hold value without the interference of any bank, govern and intermediary of any kind. "The very feature that makes blockchains so useful — their ability to enable ordinary people to transact with one another in a peer-to-peer fashion without the need for a trusted central party — also makes them vulnerable to exploitation for illicit purposes" (Maupin, 2017).

But even if the early adopters still maintain this pure vision, for business applications blockchain has to be regulated in some form. In fact, "Even well-intentioned blockchain projects can sometimes subject consumers to inordinate and poorly understood financial risks" (Maupin, 2017). In the past, governments have collaborated with intermediaries to ensure the respect for the current laws, but these same actors are the most likely to disappear in a future blockchain world.

Neither the "wait and see", nor the heavy-handed approach of banning all cryptocurrency activities seems the most useful way of proceeding. Instead, "Governments should tackle the new regulatory challenges of a disintermediated global economy by focusing on individual DLT use cases rather than their underlying enabling technologies" (Maupin, 2017).

Trying to pose limitation or excessive boundaries to the protocol development seems much of a difficult and counterproductive task, that's why regulators will probably focus on the single macro use-cases, whose boundaries are clearer, and the regulation process can be easily divided and managed in sub-tasks.

Chapter 3 – Ecosystem analysis

3.1 Introduction

Distributed ledger technology will probably innovate more than one specific sector. Its points of strength, like transparency, trustlessness and immutability are general concepts that can improve the entire spectrum of human interactions. For this reason, the types of involved stakeholders and projects created are endless, nearly as broad as for the internet revolution of the late 90's.

In the next paragraph we'll explore the major blockchain solutions currently proposed in the field of logistics and transportation, with a brief analysis of the main actors and companies behind them. Many exclusions had to be made, given the proliferation of ideas and initiatives that will probably make the entire industry flourish.

First, we'll look at the main stakeholders' classification in the space. Then we'll explore four of the most influential platforms in the space. Finally, we'll briefly cover two significant case studies that give a tangible proof of what's been made until today.

3.2 Blockchain stakeholders

From a technical standpoint, distributed ledger technology combines innovations and efforts coming from three different areas: mathematics (particularly cryptography), computer science and economics. On the other hand, we've anticipated that its applications can range from strictly monetary assets like cryptocurrencies to trust minimizer platforms for the financial, insurance or supply chain management sector.

Therefore, the spectrum of actors this technology has attracted is various and made by many types of stakeholders, of which we'll give a summarized taxonomy below:

- *Industry pioneers:* these are the actors that first dove deep into the possible applications of this new technology, trying to capture its early momentum. This group includes major technological corporations like Walmart, IBM or Intel but also thousands of startups and passionate entrepreneurs that are willing to invest time, energy and money into this new paradigm. Naturally, while they will be rewarded in case of a positive adoption of the technology, these entities accept the risk of moving too early, as well as the danger of spending a lot of resources into some venture that will deviate from what the future market's standard will be.

- *Venture capitalists:* These are participants that try to profit from this industry revolution from a financial and investing point of view. Venture capital investments in the space have grown from under 10 million dollars in 2012 to almost a billion dollar in 2017 (Rowley, 2018) (see Figure 3.1). This numbers don't include ICO valuations, whose total value raised in 2017 alone would be around 5,6 billion dollars (Williams-Grut, 2018).

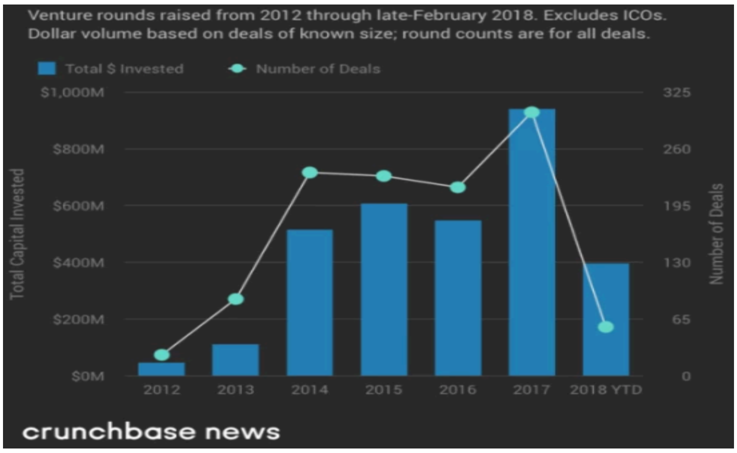


Figure 3.8: Venture capital funding in Blockchain startups in recent years (www.crunchbase.com).

- *Developers and consortia:* cryptocurrency projects (more than business blockchain ones) are mostly born as community developer initiatives. The typical software company structure is replaced by a flatter organization chart, where anyone can propose its ideas and the community adoption will judge it in a democratic way. Therefore, developers are the true innovation sources of the space, even if many other roles are needed for a blockchain company to succeed, just like ordinary start-ups. In order to conjugate pure development efforts with industry requirements and interests, many consortia have been built around blockchain in the recent years. These consortia are usually promoted and sponsored by big corporations or foundations but try to maintain an open-source and community-based DNA, in order to leave developers freely stimulating each other and independently finding the best solutions. These initiatives include the Enterprise Ethereum Alliance, Hyperledger Project, R3 and many others.

- *Academics and researchers:* the innovation in the Bitcoin space has undoubtedly outpaced the speed that researchers and academics can sustain. The Bitcoin invention itself was (probably) a private initiative, totally unrelated with the desire of creating an exhaustive publication or properly synthetize a specific subject. This said, universities will play a very important role in the future advancements of the technology, being able to use the newest innovations in cryptography, computer science and economics to solve one or more of the aforementioned blockchain limitations, that currently are the main obstacle for its adoption in the supply chain management field.

- *Governments and regulators:* especially in the logistics sector, where a great part of the value is created by international and complex business relations, regulators will play an important role in shaping the way this technology will be gradually adopted and would benefit the market. 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, Figure 3.2 shows the impact of blockchain technology at a global level, measured in the most important geographical areas according to relevance, timeliness and readiness.

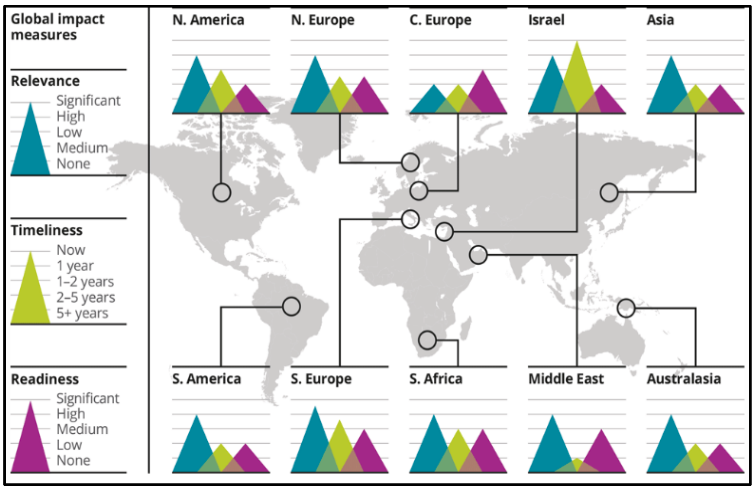


Figure 3.9: global impact of Blockchain technology (Tech Trends 2018, Deloitte Insights).

3.3 Platforms

Platforms are fundamental in every technological revolution in order to leverage the work others have already done before us and help advancing the industry. In this section, four main blockchain platforms, operating in the supply chain industry, are presented.

It wasn’t an easy choice, given that the space is not yet dominated by some clear leaders or standards. The four initiatives covered have a remarkable clear vision of what their aim is, in the field of supply chain management or logistics.

In some cases, practical evidence of successful pilot projects is cited, although we’ll examine the case studies in a more detailed way in the subsequent paragraph.

3.3.1 Hyperledger

Hyperledger is an open source project, founded in 2015 by the Linux Foundation, with the aim of supporting a series of blockchain-based initiatives and tools development. It counts now more that 100 members, including Accenture, IBM, Sap, Intel and JP Morgan. The foundation is actively trying to stimulate cross-industry collaboration on the research and development of more reliable distributed ledger infrastructures, in order to propose new solutions capable of supporting global business transactions by major technological, financial and supply chain management companies.

The project will integrate independent open protocols and standards by means of a framework for use-specific modules, including blockchains with their own consensus and storage routines, as well as services for identity, access control and smart contracts (En.wikipedia.org, 2018).

In 2016 the project began to incubate codebases from organizations members, such as the Fabric framework, proposed by IBM, or the Sawtooth one of Intel Corporation. Other incubated frameworks include Burrow, a client for the Ethereum Virtual Machine sponsored by Monax and Intel, Iroha, which is based on Fabric but has a mobile-first approach, and Indy, a side chain for improving digital identity tools proposed by the Sovrin Foundation.

Besides the mentioned frameworks, the Hyperledger project has given birth to many different tools that can help developers in the creation and deployment of a business-related blockchain application. Such tools include:

- *Caliper*, a benchmark tool that is able to test a blockchain solution against some predetermined KPIs, such as TPS (Transaction per Second) or resources utilization, before it's deployed, hugely simplifying and streamlining the testing phase
- *Cello*, a toolkit that enables "as-a-service" creation and management of blockchains
- *Composer*, which is a set of tools for simple implementation of smart contracts that allow for the use of common programming languages like node.js and CLI. It includes a rapid prototyping tool, running on the

Hyperledger Fabric, which allows the easy management of assets, participants and transactions

- *Explorer*, a blockchain module designed to create user-friendly web-applications, which can retrieve almost any information of a blockchain, such as blocks, transactions and associated data, network information (name, status, list of nodes), chain codes and transaction families, as well as any other relevant information stored in the ledger
- *Quilt*, which offers interoperability between ledger systems using the Interledger protocol (known as ILP)

3.3.2 CargoX

It is a Russian-based blockchain startup, whose mission is "to transport the global supply chain industry to the 21st century" (CargoX's Bluepaper, 2018). The first aspect of the logistic market they have decided to attack is the Bill of Lading digitization.

As we've seen, this is probably the most important document in the transportation industry. Possessing the original certificate is equal of being the owner of the goods, whose value in many cases exceeds the tens of thousands of dollars.

Given this importance, Bills of Lading are shipped from the exporter to the importer via express courier: the documents are created by the shipping carrier at the departure, then sent to the exporter, who will later forward it to the importer once the purchase terms are fulfilled (usually in case of payment from the buyer or his bank). The importer needs to send the same document, in original form, to the port of destination, because without it the goods can't be redeemed from the last mile operators. On Figure 3.3 below we can see a visualization of the flow.

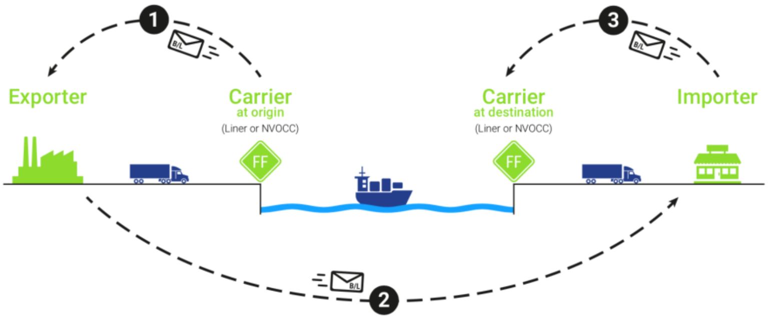


Figure 3.3: Bill of Lading creation and shipping process (CargoX Bluepaper, 2018).

This process can take up to 10 days in total, and costs 100$ on average just for its shipping, since expensive courier services (DHL, UPS or FedEx) and insurances are used. Moreover, Bill of Lading falsification is a relatively easy task, given that usually normal company paper is used for printing. Such costs for a single piece of paper can seem minimal in the scheme of a container transportation but added up they can reach more than 7 billion dollars spent yearly for the entire industry, which also from an environmental standpoint causes a useless waste of paper and significant CO_2 emissions (CargoX's Bluepaper, 2018).

There have been attempts to digitize the Bill of Lading before, such as the Telex B/L. The main differences were that central authorities were still needed to authenticate the documents, posing a significant risk of counterfeit or digital duplication of the certificates. Proprietary business initiatives like this were hard to be trusted by an entire industry as a common standard, given that the rules governing the B/L exchange processes were not transparent.

The solution proposed by CargoX aims to *tokenize* the Bill of Lading. By using a public blockchain, they can create the digital equivalent of the B/L, which they call *Smart B/L*, that is absolutely unique and unforgeable, just as a single chunk of bitcoins or an Ethereum ERC20 token. This token can be later sent from a peer to the next one, either in a manual fashion or in an automated one, using tailored smart contracts. Blockchain is therefore used as a backbone for the entire process, to which each actor refers, from the purchase parties to the logistics operators and the government institutions.

The new process structure is shown below (Figure 3.4):

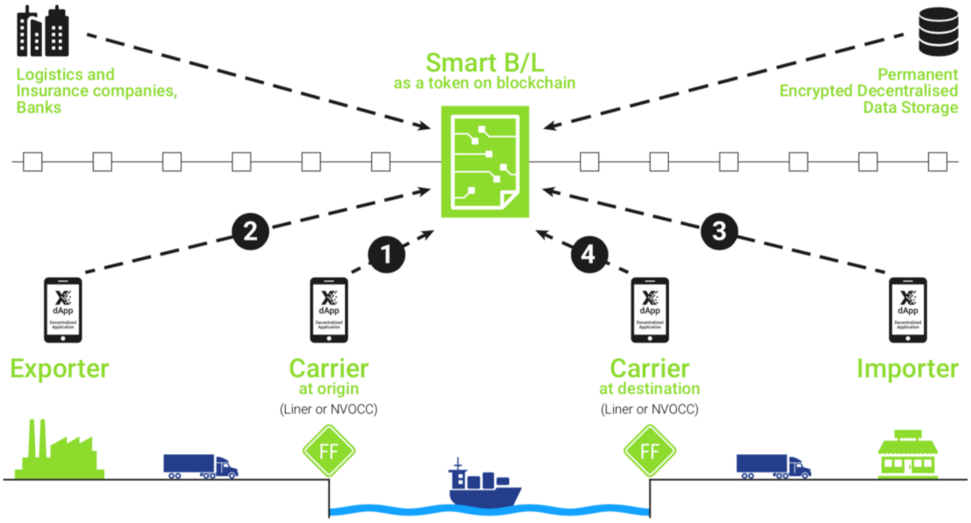


Figure 3.4: schematization of CargoX digital BoL creation process (CargoX Bluepaper, 2018).

All the stakeholders are connected to the platform through a Decentralized Application (or DApp), which they use to execute the smart contracts and retrieve the publicly encrypted data. Security and authorization of the single entities becomes possible through hardware devices with embedded key pairs. In this way, only the exporter can execute the contract that transfers the ownership of the Bill of Lading to the importer, using its own personal device, and the entire network can be assured that the operation was legitimate.

The decentralized storage service chosen is IPFS (or InterPlanetary File System), a “content-addressable, peer-to-peer hypermedia distribution protocol” (CargoX’s Bluepaper, 2018) used to store files, adequately encrypted, over a permissionless peer-to-peer network.

For their technological implementation, they have chosen a public blockchain, specifically Ethereum. The reason is divided into two arguments. First, given that the purpose of the project was to make an entire industry change its paradigm, trust was the feature to maximize. This was possible only with public blockchains, which are the most secure and reliable way to leverage blockchain technology (in fact, 99,9% of the value of current crypto-currency assets are trapped in public blockchains). This naturally comes at the expense of high operational fees, but the tradeoff seems to work since the current process imposes very high rates for Bill of Lading shipments.

Second, right now Ethereum's Turing-complete programming language is the most advanced, and its fervent community makes it possible to develop almost any kind of solutions over a system that is heavily tested by its users on a daily basis.

3.3.3 Hijro

The Fluent network project (renamed Hijro in November 2016) was founded in 2015 by Lamar Wilson and Lafe Taylor, two Stanford's dropouts who were united by the passion for decentralized technologies, especially Bitcoin. In fact, they had previously created together one of the first iOS compatible Bitcoin's wallet, Pheeva, in 2014. They later focused their attention on the blockchain technology itself, believing it could bring many advantages to a broad range of friction-oppressed industries.

They chose Supply chain finance as their niche of application, given its inefficient infrastructure, full of different individual operators and proprietary ledgers. The opacity of the current systems makes them ripe for disruption, and Taylor and Wilson firmly believed blockchain technology could be a suitable solution.

As stated in their blog, "Hijro connects banks, lenders, buyers, and suppliers to streamline and automate settlement, reduce fraud risk, and break down costly data silos in the $4 trillion open-account trade market" (Medium, 2016).

International settlements can currently take up to six days to complete, and almost 50% of US businesses still make use of paper checks, which increase latencies and costs. As a side effect, the entire process becomes opaquer also for financial institutions and auditing intermediaries that have the task of reconciling and settle them. When a wire transfer is sent, there is almost no information regarding the recipient, what goods or invoices they are for, or when the funds will ultimately be available. Moreover, this causes financing departments to become reactive instead of proactive, because predictability and forecasts are obviously limited.

The key technological aspect of the Hijro solution is the creation of so called "digital invoices", which can be bounded to physical ones in a bilateral way. This makes impossible the double spending of the same invoice (known as "refinancing") and empowers the automation and harmonization of the entire network.

Automatization of most of the working capital financing processes comes from the implementation of smart contracts that can enforce the business logics in a decentralized and secure way. Various inputs can be collected on a blockchain platform to automatically execute the release of funds or transfer of digital assets (such as receivables) allowing for a qualitatively different approach to trade that has the potential to marry information, transactions and trade contracts to provide automated real-time settlement.

Blockchain also has the advantage of being directly tied to payment channels, especially when transactions are made using their own native tokens. This allows for real-time settlements that can be approved and confirmed in seconds, with thei details openly auditable by the interested parts. Other solutions offered by the platform include a multi-bank, multi-lender Trade Asset Marketplace and a flexible working capital management solution.

The chosen architecture was a private blockchain, with a double consensus system: on the first hand, a federated structure admits only certain actors to the network, who have been previously authorized by the leaders. On the second hand, a Proof-of-Work system is put in place to guarantee an emergent consensus between the blockchain members. Although its functioning is similar to Bitcoin's mining, miners are not anonymous in this case, but instead everyone knows the nodes responsible for the data validation and the update of the shared ledger. The main advantage is that the hashing power needed by the network is much lower than in a permissionless blockchain, therefore transaction costs can be maintained incredibly low.

3.3.4 Provenance

The company was founded in 2013 by the English entrepreneur Jessy Baker, with the simple but powerful promise of "addressing the alarming lack of information around the things we buy" (Demirors, M. 2017).

People deserve a much deeper knowledge about the origin and history of the products they buy, and all the supply chain actors must be able to track the same information as the items are manufactured and shipped, without any opacity. Centralized systems can't reach this goal, given the current fragmentation of actors in the chain which also increase the risk of fraud. The truth is no one single company, even NGOs, can be trusted enough to provide the only source of product traceability: every attempt to centrally provide a unique source of truth will always be subjective to biases and inherent weaknesses.

Therefore, their focus has always been on the traceability feature of blockchains, applied mostly to consumer products and B2C companies. Alignment between business operations and environmental and social standards is also a priority, aimed at maintaining and improving ethical labor practices, environmental preservation standards, eliminate fraud and bad behaviors along the supply chains.

As described in their White Paper, they were able to combine distributed ledger technology with smart tagging, Internet of Things, new technologies of identification, etc. to track goods from first suppliers through factories and points of sales until the final customer.

Specifically, Provenance's purpose is to link every manufactured product to its digital identity, which ensures four main properties:

- The *nature* of the product
- The *quality* of the product
- The *quantity* of the product

- The current *ownership* of the product

These four properties combined define the current state of the product. When a transaction occurs, the state changes in one or more properties. All the changes are saved into the blockchain, so the complete history and uninterrupted chain of custody is publicly visible.

All the actors involved are asked to complete a registration process that links them to their key pair, which is adequately authorized to submit changes in the product state, depending on their nature (whether they're producers, manufacturers, auditors, and so on). This registration process doesn't undermine the anonymity needed in many supply chain applications, but at the same time gives certainty to the network that only the allowed participants can change the product's state, just as nodes in the Bitcoin network can validate other peers' transactions, even without knowing their identity.

Production programs can be used to prove the creation of the products, that happens simultaneously with the creation of its digital state. Some of the parameters needed for such operation are the exact quantity of goods created, the specifications (also called "tags", that describe its attributes like organic, fair trade, etc) and the financial value and/or price of the items. Production programs can be audited and revoked if suspect of illicit activity arises.

The implementations used by following actors in the chain, that turn the raw goods into finished products, are the *manufacturing programs*. Any user authorized to use such programs can submit transactions that change some properties of an item's state.

Blockchain makes possible to check that no quantities are created or destroyed by manufacturing programs: every unit of product created by production programs must have a history that has an end, even if it's wasted or thrown away. Because of its auditability, the blockchain provides the same cast-iron guarantee as in the physical world; namely, that creation of an output good can happen if and only if the required input is used.

What we previously called *tagging* is the act of linking a physical product to its digital counterpart. Provenance uses a broad range of sensors and instruments to achieve this goal: from barcodes to digital tags of RFID labels.

For a user-friendlier experience, all of Provenance pilot projects involve the creation of a consumer mobile application that can be used to scan a product's code and retrieve its complete history in a visually compelling format. This combination of a simple frontend infrastructure combined with a trustful and decentralized engine can make a difference in modern supply chains.

3.4 Case studies

Even though, as we've repeatedly stated, blockchain technology is still living its infancy years, especially from the point of view of its technological capabilities, some notables pilot projects have been successfully deployed, either by big corporations and by new and bold startups.

In this paragraph we will examine two case studies:

- The first consists in a platform for global logistics management, created by a collaboration of IBM and Maersk, one of the leaders in the shipping industry

- The second is a project developed in the Indonesian fishing industry by the blockchain startup Provenance, one of the most interesting among its contemporaries

3.4.1 IBM and Maersk

In January 2018, Maersk and IBM announced the intention to establish a joint venture to provide more efficient and secure methods for conducting global trade using blockchain technology (IBM FinTech: Asia, 2018). A new company will be founded, with the aim of creating an open platform that will provide useful services and digital integrations.

The analysis they run estimated a total cost for global trade approaching 1,8 trillion dollars every year, with potential savings amounting to approximately 10%. Needless to say, the complexity of the entire sector is steadily growing every year. Ocean freight covers the most part of the goods transported: apparently, of the 4$ trillion valuation of goods shipped every year, 80% are loaded on maritime means of transport.

Trade documentation makes a significant cut of the total shipping costs: in some cases, in fact, documentation expenses reach 20% of the entire spending budget needed to move the freight to the destination. As previously anticipated, logistics supply chains are heavily affected with trapped value, and the potential savings are quite astonishing, both in percentage and in absolute means.

The solution the propose is a platform, capable of leveraging blockchain technology to minimize the trust that today is needed and paid, in order to make all the different and fragmented stakeholders work with each other. Today's logistic supply chains can be over-simplified with the following illustration (Figure 3.5):

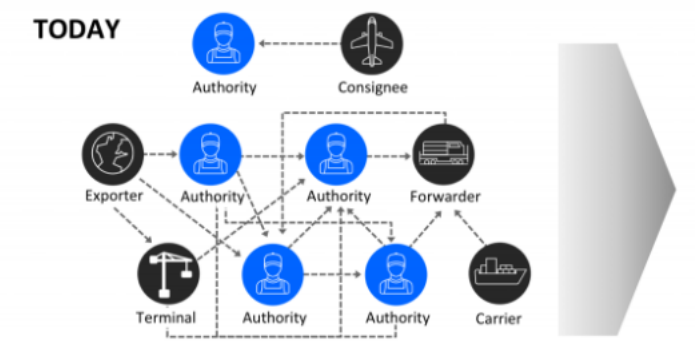


Figure 3.5: the AS-IS process (IBM website).

Many of the aforementioned issues can be inferred, looking at this process mapping:

- The relationship between the different actors are really complex and intricate. This in turn makes lots of continuing reconciliation and alignments needed, which are costly and increase the possibility of errors and misunderstandings.

- Data is not easily shared with peers. Data silos characterize the entire supply chain and are responsible for slow process advancements and cumbersome procedures.
- Manual and paper-based processes are needed, that add complexity and probability of mistakes.

The decentralized platform will act as a foundational layer, on top of which all the relevant information and documentation will be based (see Figure 3.6).

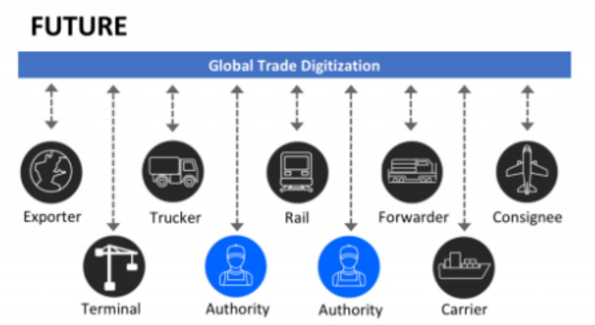


Figure 3.6: the revisited process (IBM website).

A single and trusted source of truth will bring huge improvements on all the covered areas and problems, in particular:

- Every stakeholder will be able to autonomously verify the authenticity of the data. No more data silos will be present, but instead all the information will be available through the distributed database. While making openly visible to everyone the fact that some piece of information has been added to the blockchain, and preserving the immutability of the same data, the technology allows for selective encryption of it: it means that every actor can verify that the information has not been changed, but only the authorized partners can see the actual data: this is important because in such complex supply chains, privacy of companies' trade secrets is one of the critical success factors.

- Trust will be heavily improved over the traditional flow. None of the actors will be forced to trust any of the other partners, thanks to the blockchain foundations of the network. This will remove the hefty fees normally paid to central intermediaries (banks, financial partners, insurance companies, government's institutions) that today are mandatory in such types of global trade networks.

- No system or solution is perfect: blockchain will definitely decrease the failure rate and minimize the number of mistakes and frauds occurring, but it won't eliminate them. However, by having a complete and trusted track record of all the relevant documentations and events, many operations such as risk assessment, dispute resolution and interventions can be simplified by orders of magnitude.

The platform will be built on top of existing IBM Blockchain and Cloud technology but will have its foundations on the opensource project Hyperledger. Naturally IBM will use the Hyperledger Fabric 1.0, which they have heavily sponsored from the beginning.

The platform will bring innovation and advantages to the entire network, including not only clients and suppliers, but also freight forwarders, port and terminal operators, customs authorities and individual shippers. The benefits for each actor are summarized below:

- Ports and terminals: with reliable and updated information on the freight, ports and terminals can improve the planning of import and managing activities, reducing the total lead time and thus increasing containers throughput rate

- Ocean carriers: real time access to end to end supply chain events can benefit ocean carriers, making the relationship with the ports easier and leaner, saving route planning and port activities time

- Customs authorities: clearance activities can be heavily reduced thanks to the digitization of the previously paper-based documentation. Risk assessment can be simplified, given the reliability of the data and the integration with national and international platforms

- Freight forwarders: updated and reliable data on individual shippers can benefit freight forwarders in the arranging of each shipment. At the same time, being able of always tracking each single container would bring enormous advantages to forwarding partners, dramatically improving the service level they could offer to their clients

- Individual shippers: greater predictability will facilitate the daily operations of independent shippers. Other benefits include the earlier notification in case of issues, that can be therefore tackled in a faster and better way, full transparency in terms of fees due and less safety stock inventory

Since the collaboration started in June 2016, multiple parties have piloted the platform including DuPont, Dow Chemical, Tetra Pak, Port Houston, Rotterdam Port Community System Portbase, the Customs Administration of the Netherlands, U.S. Customs and Border Protection (White, 2018). Moreover, the list of interested partners is growing on a daily basis, confirming the interest of a broad range of actors towards this kind of solutions.

The platform is still in a closed beta phase, its launch is currently estimated for the Q4 of 2018.

3.4.2 Provenance (Indonesian tuna fishing industry)

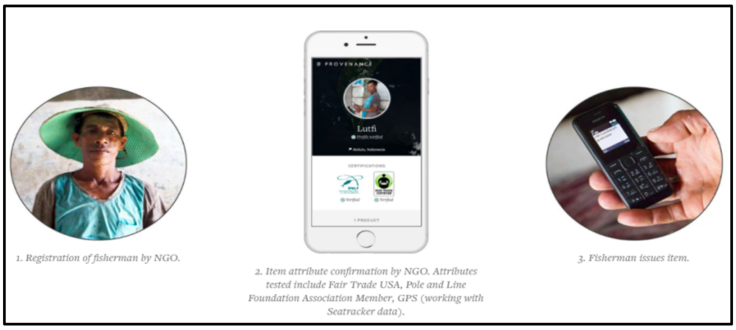
We've already mentioned Provenance as one of the most interesting start-ups in the blockchain space. Their most famous pilot project, which is probably one of the most successful implementations of blockchain in a supply chain environment to date, consisted in creating a traceability program for the

Tuna fishing industry in Indonesia, currently compromised by human rights abuses, overfishing, fraud, illegal, unreported, and unregulated activities.

Provenance worked very closely with all the relevant industry members, from fishermen to engineers, Quality assurance officers, local and global fishing associations. 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. The instruments used to acquire and manipulate the data were quite old-fashioned, from pen and paper to simple excel files or iPad forms filling.

The company leveraged the fact that all fishermen had access to a mobile phone and a 3G connection, even if patchy, to put in place their registration program: every worker was given a unique digital identity, linked to a key pair embedded in his local application (shared with no other device). The data gathered by Provenance is monitored by some external NGOs that certify the minimal environmental and social conditions of the workers, relatively to industry and fair-trade standards.

Once the fisherman catches a tuna, he just sends an SMS with the minimum requirements of the product, which activates a smart contract that "creates" the digital tuna on the blockchain and sets its ownership to that same person. Every item is identified by a permanent and unique ID the asset can be now transferred from the fisherman to the first supplier, physically but also digitally (see Figure 3.7).



1. Registration of fisherman by NGO.

2. Item attribute confirmation by NGO. Attributes tested include Fair Trade USA, Pole and Line Foundation Association Member, GPS (working with Seatracker data).

3. Fisherman issues item.

Figure 3.7: creation of a product specific entry on the blockchain (www.provenance.org).

The advantage of using a public blockchain like Ethereum is that everyone is able to view the data independently, even without using the Provenance application. Every transaction can be retrieved from any web explorer (like EtherScan.io) giving maximal traceability and visibility to the process. All the state changes (represented by Ethereum transactions) are inherently timestamped. That means that completely immutability is guaranteed, changing or deleting past events is impossible for any actor.

When the fish will be sold to the next supplier, both parties will sign the digital contract with their private keys to authenticate the transaction. 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.

When tuna is later transformed in the factories, manufacturing programs are used in combination with smart devices that can trigger the data entry on the blockchain. For example, 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. Provenance has programmed the mass balancing machine with the precise instructions that a can of Fair Trade skipjack tuna contains 200g of tuna and 10 ml of olive oil; if the required ingredients are loaded on the weight scale, a transaction will be generated, which changes the state of that piece of the initial product to a different digital entity, representing the single can. Unicity of the tokenized information on blockchain ensures that the system cannot be tricked to believe more tuna exits the factory, relatively to how much has entered. Moreover, even if new assets are created, their link to the previous state is immediate to retrieve from the ledger.

Blockchain acts as a layer on top of existing information systems, without eliminating them. Every transaction will be recorded also in the proprietary systems of the involved companies, for a simpler data manipulation, but their accuracy can be always checked against their equivalent on the ledger. The can will be equipped with a simple QR code that, if scanned from the Provenance App, will query the item’s history of the product in a matter of seconds, maintaining at the same time high levels of reliability.

Chapter 4 – Case Study: Luxottica and the Current Process

4.1 Introduction

In the previous chapter the main applications of Blockchain Technology in transportation and logistics have been listed and analyzed, trying to underline their potential benefits for the industry, as well as the limitations that need to be overcome. The aim of the next two chapters is to synthetize what has been learned from the state of the art into a practical case study, proposing an alternative blockchain solution to the current logistics process of an operating company. The study has been developed during an internship at Luxottica, a leading reality in the eyewear and sunglasses market, whose main logistics hub is located in Belluno, Italy.

In particular, the role was in the Oakley AFA International Logistics team, responsible for the transportation of the AFA products (Apparel, Footwear and Accessories) of the American brand, from the factories of the Vendors that produce the goods to the six different distribution centers, located all over the world. The logistic unit was brought in the Italian facility less than two years ago and since then has undergone a significant amount of automation and integration with Luxottica's already proven systems. The internship enabled the understanding of how processes were managed before the integration, in a highly manual way, and how automation and synergies with the other company functions and the Vendors network can improve the overall efficiency and success of the entire business.

4.2 The company's history and business model

Luxottica is the market leader in the eyewear and sunglasses market. Its dominance in the design, production and distribution of luxurious and sport frames made it the most profitable company in the Italian fashion industry in 2012 (Luxottica, 2017).

Founded in 1962 by Leonardo del Vecchio, at the beginning it only did mechanical treatments for other businesses, but subsequently followed a vertical integration strategy with the aim of controlling the entire supply chain, from the production of the frame to the final sale, including all the logistics aspects.

The design, together with the samples development and the actual industrialization, takes place in the original facility in Agordo, a little town near Belluno, Italy. The other productive facilities are located in Italy (five locations in Cencenighe, Rovereto, Lauriano, Pederobba and Sedico), in China (three in Guandong), one in Brazil, one in India and one in Foothill Ranch, California, acquired in 2007 with the Oakley brand. The Group sells its products in more than 150 world countries; on more than 50 of them proprietary offices have been opened. The company has gained fame for the "Welfare" its employees benefit from, such as life insurance discounts, scholarships, textbooks for employees' sons, counselling (Ganz, 2017).

The winning strategy for Luxottica has been, without any doubt, the *vertical integration* it has always promoted. As mentioned early, this kind of internal synergy between functions can be found in every aspect of the business, not only tied to production and logistics, but also sales, customer service, IT departments and HR forces.

4.2.1 The history

What follows is a brief history of the critical steps that made the transformation of the little laboratory into an industry giant possible.

The beginnings: Leonardo Del Vecchio was born in Milan and, after his father premature death, was raised in the Martinitt orphanage. As a young kid he has always been passionate of manual and precision activities, training himself in multiple little shops around the city. Not much after completing his studies, he decided to accept one of the multiple grants that the Agordo town was giving to young entrepreneurs that wanted to bring there their activities. The company continued working as a service provider for other local businesses until the end of the '60s, fabricating mainly mechanical components for the eyewear industry (Brunetti and Camuffo, 2000). In 1966 the employees count started to approach the 70 mark.

The next year, in 1967, Del Vecchio started to produce and commercialize his own glasses brand. The two original partners, Toscani and De Cortà, didn't agree with the choice and asked for a liquidation of their shares, which they obtained after some difficult negotiations. It's worth mentioning that at the beginning of this new phase, given the poor financial conditions of the business and the only remained founder, the entire family gave its contribution to the actual production of the frames. Del Vecchio personally worked on the aluminum junctures, while the wife and kids would pose the color on the frames. The father drove every day to Milan at night to deliver the finished products and be back the following morning for his production turn (Stella, 1996).

The internationalization and the integration: In 1971 Luxottica attended the MIDO (the international eyewear fair in Milan) for the first time, presenting an entire collection of proprietary spectacles that had great success among big distributors and opticians. Sales started gaining momentum and the process of internationalization began, even if only through distributors.

Del Vecchio started seeing the disadvantages of a disintermediate supply chain, in which he couldn't directly reach his final customers. The first step taken to overcome this situation was the acquisition of the company Scarrone from Turin, responsible for the commercialization of the Luxottica brand in the entire Italian Peninsula.

During the ‘70s the company grew both in terms of personnel and revenue. It broadens its production line, from only metal frames to a collection of metal, plastic, sun and eyewear offerings. This initiative was fueled by the market preference for plastic sunglasses that started taking off in the second half of the decade; the transition wasn’t easy, and one of the worst occupational crises of Luxottica’s history took place in 1979.

The ‘80s - continuous growth: Luxottica Group S.p.A., the holding company that owns all the business-related participations, was created at the beginning of the ‘80s. In order to increase the direct contact with the leading markets, new branches were opened in Germany, Spain, UK, France and Sweden. In 1982 Luxottica acquired a consistent participation in one of the leading eyewear distributors of the time: Avant Grade Optics. In the same year, a new commercial entity was created with a Venezuelan oil merchant, the Berdel Inc. (Brunetti and Camuffo, 2000). These two operations gave Luxottica the leadership over the US market, with a total reach of 7%.

The second half of the decade consecrated the spectacles as a truly fashion item. Before then eyewear frames were related to shame in most cases, representing only a remedy for a health deficit. Luxottica cleverly started licensing the frames’ production of some of the most famous fashion brands, fabricating the products of their lines in exchange of a royalty for every piece sold. The most important deal was made with Giorgio Armani, who became shareholder with a 3% participation, in exchange of the license for its brands collections. At one moment, the revenue of the Armani collections counted for 50% of the total revenue of the group. It’s worth noting that this type of dependency to a single client in not uncommon for today’s eyewear production companies, but Luxottica never returned to that state again.

The ‘90s: the IPO and the Ray Ban acquisition: In 1990 Luxottica was listed on the New York Stock Exchange. It was the first case of a company conducting an IPO in a foreign country, without being already listed on its national market. The choice was made in order to increase the visibility of the company that was still unheard, even though already the market leader. Among the strategic advantages of the operations we can list:

- New capitals could flow in and sustain the heavy acquisition strategy planned to follow the integration and the expansion on new markets.
- The company officially entered the international stage, with all its related logics, stepping away from the limitation of a family business.

The expansion in Europe and in the rest of the World continued (the most notable opening was in Brazil) with new branches created and new brand licensed (most notably Vogue and Persol). The first production plant in China was built and the company entered the Retail business acquiring the US Shoe Corporation which owned Lens Crafters, the biggest retail chain for opticians, together with a shoes production division that was later sold.

The most important event was without any doubt the acquisition of Ray Ban in 1999, optical division of the Baush & Lomb group. This operation enabled the rise of the sunglasses business for Luxottica, while it strengthened the marketing and branding abilities of the company, skills that would later pay an important role in shaping some of the most iconic frames of all time, like the Aviator model (Repubblica, 1999).

The '00s, continuing expansion: In the year 2000 the company got listed on the Milan stock market. The new market would grow in percentage of shares traded, until in 2017 Luxottica was de-listed from the NYSE, representing at that point only the 3% in volume (Luxottica, 2017). In 2001 Luxottica acquired Sunglass Hut, one of the leading retail chains in North America, Australia and the UK. Sunglass Hut would grow inside the group to become the first retail brand for the commercialization of medium-high class frames. Other notable achievements of this decade are:

- The invention of the STARS program (Superior Turn Automatic Replenishment System). It consists of an information system that enables new synergies with the wholesale client. The model used is the "Vendor Managed Inventory" one, where Luxottica manages the stock of the client, taking full responsibility over the replenishment process. Some of the advantages of this program are:

  - A better product selection for the final customer
  - A continuous turnaround of the offerings
  - Automatic replenishment
  - Better collaboration with the marketing efforts, that can be centralized and done inside Luxottica for all its clients
  - Stock optimization, on the basis of seasonal trends and store profiling
  - Increased "go-to-market" speed, promoted by the enhanced order reactiveness
  - Sales increase (up to 25%, relatively to a baseline of 8-10%) (Lucchetta, 2016)
- The acquisition of OPSM (Optical Prescription Spectacle Makers) in 2003, an important Australian chain, always famous for its focus on the customers
- The expansion on the Retail market in 2004 with the acquisitions of Pearle Vision, Sears Optical and Target Optical
- The entrance in the Chinese market in 2005 with the acquisition of Xueliang Optical, Ming Long Optical and Modern Sight Optics. These retailers have been together re-branded into the Lens Crafters chain, now the biggest optical retailer in the Chinese market
- The acquisition of Oakley in 2007, which declared the entrance of Luxottica in the sports and high-performance American market. For the first time one of the brands acquired by Luxottica was also producing clothing lines. The two companies remained physically separate until 2017 (Sacchi, 2016)
- The creation of a separate no profit organization OneSight, with the aim of giving optical services and prescription to the ones that cannot afford it, given that is estimated that one in every seven people currently can't have access to specialized medical examinations and buy a frame. Luxottica doesn't only use financial resources to achieve this goal, but

also intense marketing and communication campaigns. Employees can also offer their help in some of the physical locations where the association operates

- In 2008 Luxottica enters the e-commerce ecosystem, selling directly to the final customer through its brands' websites. (RayBan.com, Oakley.com and SGH.com), offering also the possibility of customizing the frames (RayBan Remix and Oakley Custom)
- In 2011 the expansion in the Latin America continued with the acquisition of Multiopticas Internacional, the holding company behind one of the biggest South American retailers, GMO (Luxottica, 2017). The acquisitions of Tecnol, with its strategic distribution network, and Oticas Carol, one of the biggest franchising chains in Brazil, would follow
- In 2016 the company acquires Salmoiraghi & Viganò, one of the most important Italian retailers with over 430 locations, in order to strengthen its position in the Italian market
- New brands were licensed, including Chanel, Prada, MIU MIU, Versace, Donna Karan (DKNY), Dolce & Gabbana, Burberry, Paul Smith, Ralph Lauren, Tiffany, Tory Burch, Coach, Starck Eyes, Michael Kors and Valentino
- On January 15th, 2017 Luxottica and Essilor, the leading global lenses manufacturer, announced that they will merge, creating one of the global leading players in the optical sector, with more than 140'000 employees, branches in 150 countries and over 15 billions in revenue (Adkronos, 2017)

Figure 4.1 includes some of the most famous brands currently owned by the group or licensed.

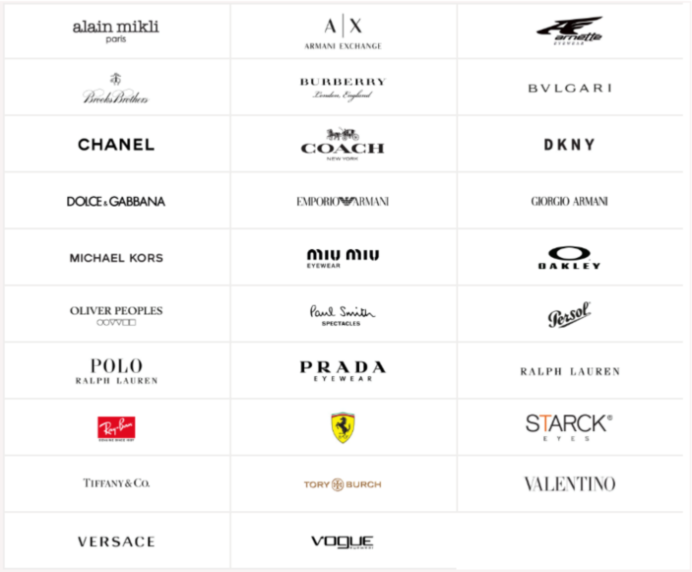


Figure 4.1: some of the brands whose production is made by Luxottica Group (Luxottica website, 2017).

4.2.2 The business model

The most important aspect of the company's strategy is the vertical integration it has pursued since the beginning, under the leadership of its founder and president to date. The reasons behind that lay in the advantages such an integrated structure can bring. The effects are mostly visible on the distribution network, which hasn't been possessed by Luxottica only for a short period at the beginning of its growth. For the wholesale market the strategy has been to open many branches in the main countries it wanted to serve, while for retail the numerous acquisitions enabled a capillary growth of its network.

The desire was to better understand the customer and his needs, in order to be able to satisfy it in the shortest time possible. For instance, when in the '80s sunglasses started emerging as a fashion item, the strategy pivoted towards strong acquisitions and licensing of famous and iconic brands.

Needless to say, an effective integration of the logistic supply chain enables the creation of important synergies that bring economical savings and improved efficiency and efficacy, in terms of service levels.

In the next figure (Figure 4.2) the main internal processes of Luxottica are detailed, demonstrating that the company has successfully integrated all the manufacturing and logistic phases of the supply chain.

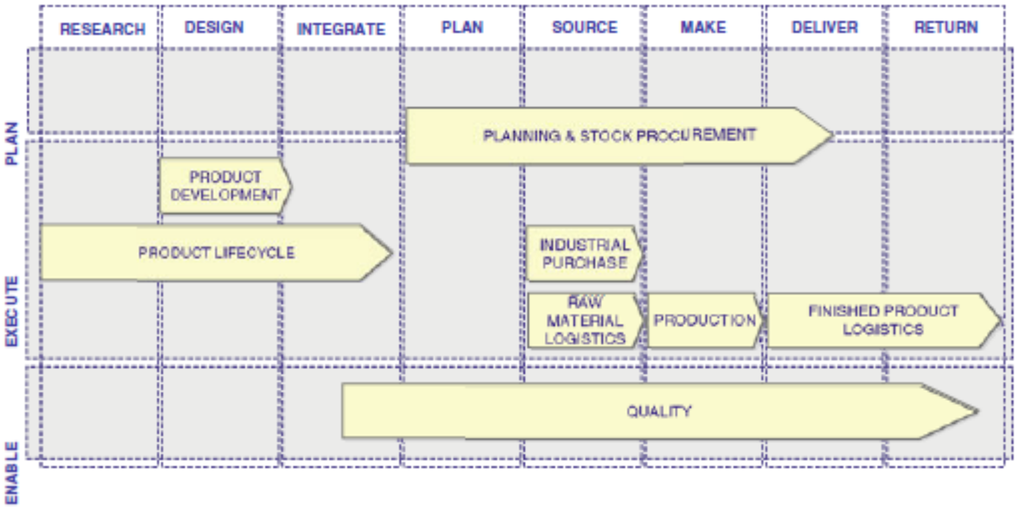


Figure 4.2: the main processes inside Luxottica (Tonchia & Quagini, 2010).

Among the advantages of such a structure we can find:

- A substantial improvement in terms of production cycles efficiency
- Direct control of the entire production, which leads to an easier and more reliable quality control over the entire product lifecycle
- A more rapid introduction of innovation, when needed

While on the distribution side:

- Products can be offered in all the most developed markets (especially the US)
- A direct contact with the final customer can be established
- Trends can be spotted in advance, instead of only going through distributors for the sales of the products

The group has always used acquisitions to increase the value of the partnerships for both sides, and all the companies that were bought saw in Luxottica a partner to scale their business, more than a simple buyer, not only from a financial standpoint, but also from an image and branding one.

4.2.3 The logistics system

As we've previously mentioned, the company currently sells in more than 150 countries, so a strong and robust logistics network is needed to serve the clients in the best way possible. The value and fragility of every single frame makes it difficult to move in bulk without the right caution. The direct control on the distribution process allows for a reduction of the supply chain's lead times, as well as an increase on the service level and perceived quality for the customers.

The logistics processes are managed by an integrated information system, shared by all the facilities of the globe. A central department analyses the sales trends and the stock levels on a daily basis, in order to keep the demand of all markets satisfied in the less time possible. If the demand is monitored constantly, the final retailer can keep inventory at minimum and costs lower as a consequence.

The distribution system is one of the most advanced in the world, composed by 12 different distribution facilities around the world that directly serve the two sales division of the business, wholesale and retail, as well as the new ecommerce flow. The distribution centers are organized in two levels:

- *Primary hubs*: they are located in strategic areas to serve the main markets and are also responsible for the replenishment of the secondary hubs. In this category we find:
    - Sedico 1 (Italy): it ships the total Italian production from the six productive facilities (Agordo, Cencenighe, Sedico 2/3, Pederobba, Rovereto, Lauriano) to the other facilities of the Group. The markets served are Europe, Middle East, Africa and some particular locations in the United States. It is the biggest logistics center, with more than 240.000 units shipped daily (Luxottica, 2016)
    - Dongguan (China): It receives the Chinese production (almost 40% of the total production of the business) and can ship up to 200.000 pieces per day. It serves the regions of APAC (Asia

  Pacific) and after the closing of the local warehouses in Japan and Australia, also their markets
  - Atlanta (US): receives the production of Oakley. It serves the North American market, the most important for the brand. With its 160.000 count of potential daily capacity it is the third biggest warehouse of the group
  - Jundiai (Brazil): it serves the local market in Latin America, shipping the production of the Campinas factory (about 3% of the group's total one)

- *Secondary hubs*: these warehouses are replenished by the primary ones, forming a global net that allows for a fast and lean distribution of the frames to the final customers located in every market. In the recent years Luxottica has started to close some of the secondary hubs and to serve the clients directly from the primary ones, improving the service levels of the forwarders for the direct shipments. By eliminating the intermediary destinations, some advantaged arise, like:
  - Cost reduction in the warehouse's management
  - Significant stock reduction
  - Delivery schedules more reliable and generally faster

There are now 8 secondary hubs, located in every continent and replenished on a weekly basis by the primary hubs. In the next figure (Figure 4.3) we can find a schematic map of their locations and main properties.

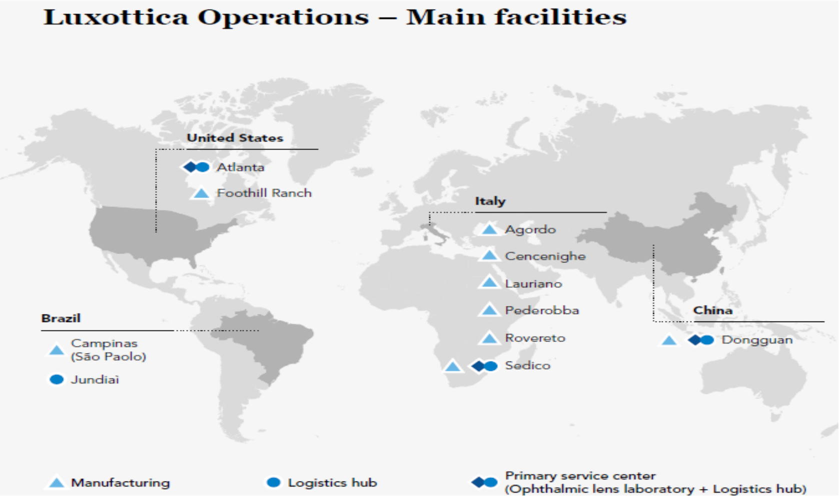


Figure 4.3: Main logistics facilities of the group (Luxottica, 2016).

4.2.4 The AFA business

As we've previously anticipated, on June 2007 Luxottica acquired the iconic Californian company for an estimated 2,1 billion us dollars, corresponding to a price of $29,30 per share (Luxottica, 2007). Oakley was a global leader in sports performance optics in a wide range of forms, including sunglasses, goggles and prescription lenses. The brands controlled by the group were numerous, including Oliver Peoples, Paul Smith Spectacles and Dragon. In addition to its global wholesale business, the company has pursued a retail strategy acquiring some chains like Bright Eyes, Sunglass Icon and The Optical Shop of Aspen and opening its branded shops Oakley Stores.

The group also offers a wide collection of apparel and accessories products, not related to eyewear. This division is called AFA (Apparel, Footwear and Accessories) and it is currently the only case inside Luxottica Group where non-eyewear products logistics supply chain has been completely integrated inside the company. The business unit currently grosses more than $250 millions in revenue, selling through more than 900 stores all over the world.

The goods are produced externally, from a network of about 50 vendors, mainly located in South-East Asia and Latin America. This is the only area of

Luxottica's holding group where the goods are not (at least mainly) produced internally. In Figure 4.4 we can see the main locations of the vendors facilities.

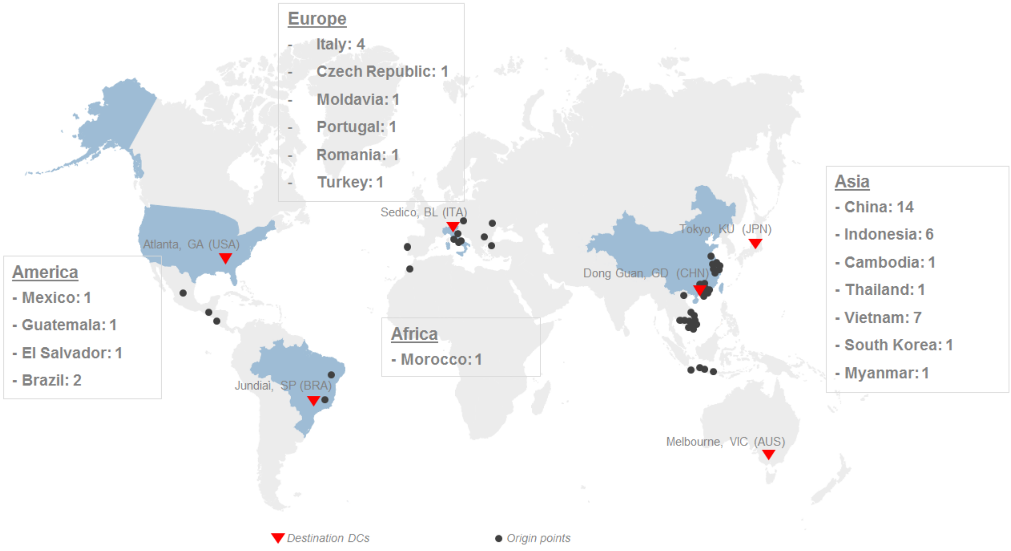


Figure 4.4: Vendors facilities locations and general statistics.

The products are sent to the 6 main hubs, each one operating in its geographical area. The main continent for sales is North America, which counts for 60% of the total sales. Europe and Japan follow with respectively 11% and 10% of the total revenue.

All of the supply chain departments are located in the Milan headquarters, except for the logistics team that is based in Sedico, close to the logistics heart of the company. While the entire eyewear production is made in facilities directly owned by the company and transported to the nearest logistics hub with stable and consolidated processes, for the Oakley AFA business an additional network has to be managed. The products need to be shipped from the vendors to the 6 hubs, coordinating all the actors involved in the international shipments.

All the planning activities depend on the market demand, which is served in two distinct periods of the year, the Spring/Summer and the Autumn/Winter season. Every season is further divided into four or five milestones, called "drops", by which specified quantities of materials have to reach the final stores. There are also some capsule collections that can be arranged independently from the seasonal production, mainly inspired by some special collections and shipped with high priority. Figure 4.5 shows the quantities shipped for each one of the five drops of the last Spring-Summer collection, while Figure 4.6 highlights the recent main capsule collections shipped.

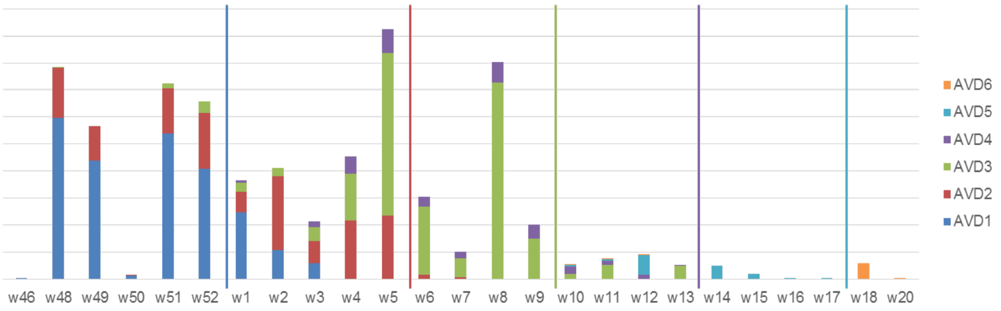


Figure 4.5: SS18 drops calendarization and quantities.

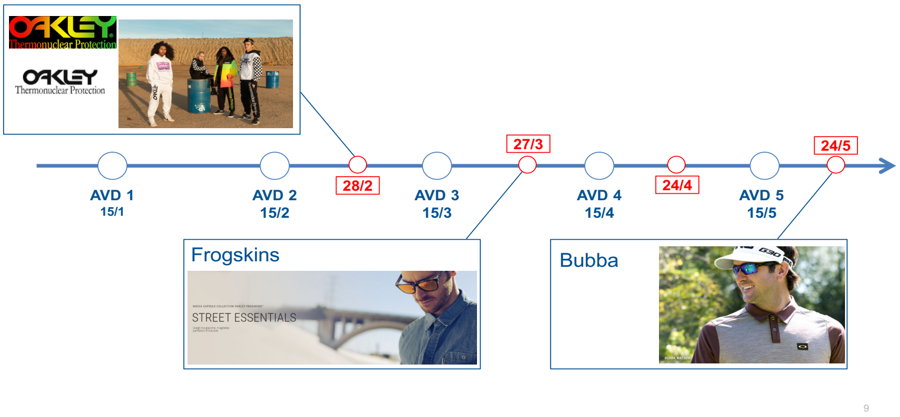


Figure 4.6: main capsule collections of early 2018.

The sourcing team is responsible for the commercial negotiations with the vendors, as well as the agreements over quality and operational standards. It directly manages the contacts with all the vendors, except for a large portion of the Asian ones, which are managed by an intermediary partner.

The planning and procurement teams schedule the production and transportation lead times and deadlines, starting from the aforementioned drops and retro-planning from them. Materials are combined into Purchase Orders (PO), progressive numbers that should be the fundamental unit of transport also for the logistics team. Below, in Figure 4.7, the structure of the AFA supply chain is shown in general blocks.

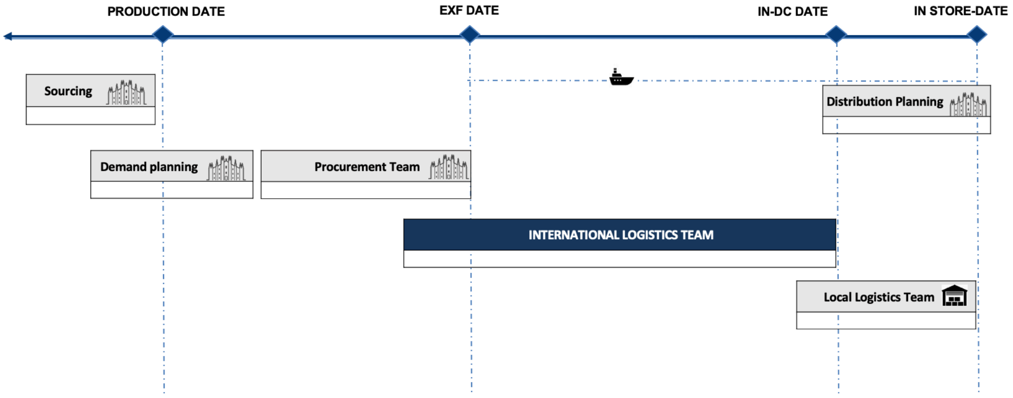


Figure 4.7: Supply chain actors and timeline in the Oakley AFA business unit.

A Purchase order collects a list of materials, defined by an UPC code that is unique for every combination of style, colour and size. For each UPC a scheduled quantity is planned, and the sum of the quantities adds up to the total purchase. The PO is related to a set of dates, which are the same for all the materials included. These dates are:

- The *Ex-Factory date*: the date on which the goods have to be available for the pick-up by the shipper. In case of EXW incoterm, the materials must be collected in the outbound zone of the vendor's facility, while for FOB shipments the Ex-Factory dates coincides with the date of materials availability at the origin port (or airport)
- The *Statistical Ex-Factory date*: at the beginning of each season, when the POs are created, this date coincides with the Ex-Factory date. Because unexpected events may happen, or new business decision may arise, this date can be changed, normally with sufficient notice. However,

what changes is only the Ex-Factory, while the Statistical Ex-Factory date always remains the same

- The *IN-STORE Delivery date*: this is the date by which the goods have to reach the final store, as decided from the business. This is the most important date, because it is strictly related to the sales each store can complete, and consequently the revenue it can generate. The date is usually scheduled for replenishment reasons, based on the sales forecasts of the stores, whose stocks have some buffer. However, for capsule collections (that most of the times have scheduled campaigns and launch events) and special periods like the "back to school" month in August, not respecting this date can seriously damage the profitability of the business, so particular attention is paid
- The *IN-DC Delivery date*: even though the IN-STORE Delivery date is crucial for the business, it is not directly under the responsibility of the International Logistics Team in Sedico, whose job ends when the materials reach the Distribution Centre. Every DC will then have its target times for the allocation and shipment of the orders, with a little buffer, but respecting the IN-DC Delivery date is really important for the international logistics.
- The *Statistical IN-DC Delivery date*: as for the Statistical Ex-Factory, it cannot change and it's the last day on which the shipments must arrive at destination. It can be different from the IN-DC one since the starting of the season, because the last one is calculated by adding the target transit times to the Ex-Factory date, while the Statistical one is based on market and business dynamics.

Moreover, for each PO a unique *Incoterm* is negotiated with the vendor, and a standard mode of transport is chosen, based on the aforementioned dates compared to the transit time of each available mean of transport.

The International Logistics team, in which the internship has been made, directly manages the shipment of each PO, starting from the communication of the goods' readiness by the vendor, until the materials reach one of the DCs, where the local import team will manage the inbound operations. The job requires analytical skills for decision like the mode of transport to use to minimize costs, or the consolidation procedures that can be made with the shipments from other vendors of the same area, as well as operative and soft skills in the daily contacts with vendors, forwarders and shippers.

For this case study the transportation of an FCL (Full Container Loaded) is analysed. First, the AS-IS procedure will be described below. Thereafter, a solution proposal based on a blockchain technology infrastructure will be detailed in the next chapter. The promises of such a solution will be checked against a set of operational and financial KPIs, and final conclusions will be made.

4.3 The AS-IS process

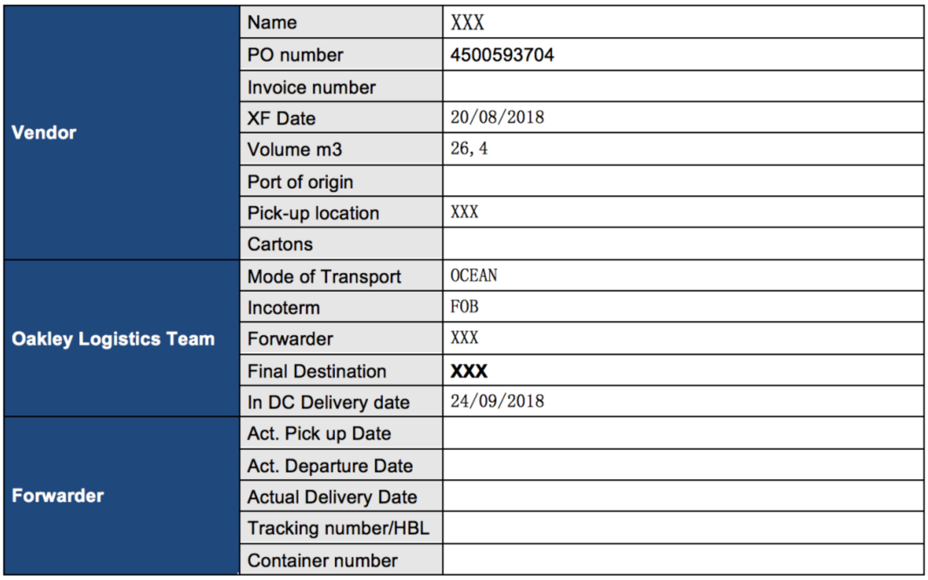
Ideally one week before the planned Ex-Factory date, the vendor sends to the Oakley International Logistics Team (which from now on will be called *the Logistics Team*) the relevant documentation about the freight that will be shipped. This documentation must include:

- A *preliminary packing list*, detailing the exact material quantity for each SKU, as planned with Oakley's procurement team. Pieces of the same material, size and colour can be grouped, for simplification purposes. The packing list should also contain some invoicing information, like vendor denomination and VAT number, as well as the address of the manufacturing facility. Most of the times it contains also a description of the packaging type and units that will be used to transport the goods, which can be pallets or (most of the times, especially for Asian vendors) cartons.

- The *commercial invoice* for the shipment. This document is optional (as long as the financial information is present in the preliminary packing list) and must contain the prices for each item, as well as the total amount charged for the freight in the local currency and, if possible, in US dollars. The invoice has validity only if the packing list is already in its final draft, and no item will be changed.

Once the Logistics Team receives the documentation, the phase of shipment’s approval take place. First, the correctness of the information provided is checked: the total shipped quantity must be the same of the scheduled quantity, within an acceptable error range. Shipping quantities greater (overages) or smaller (shortages) that the planned ones are generally accepted, under the aforementioned boundaries, because the Vendor usually produces the goods in production lots, that can be slightly different from a divider of the scheduled quantity.

Secondly, an approval template is sent to the vendor (replying to the original documents) and the relevant logistics actors in copy. A typical approval table is shown below in Figure 4.8:



Vendor	Name	XXX
	PO number	4500593704
	Invoice number	
	XF Date	20/08/2018
	Volume m3	26, 4
	Port of origin	
	Pick-up location	XXX
	Cartons	
Oakley Logistics Team	Mode of Transport	OCEAN
	Incoterm	FOB
	Forwarder	XXX
	Final Destination	**XXX**
	In DC Delivery date	24/09/2018
Forwarder	Act. Pick up Date	
	Act. Departure Date	
	Actual Delivery Date	
	Tracking number/HBL	
	Container number	

Figure 4.8: an example of an approval table for a shipment.

Let’s look at the information provided one by one:

Vendor denomination and address: especially when the shipment will be arranged by an external forwarder, the vendor contacts are important to make the interaction between the interested parties possible.

Purchase Order number: given that email is the chosen medium for the approval process, it’s important to mention the PO number in the same table, as it will make the research in the inbox easier in the future. PO numbers should be fulfilled in one single shipment, making them a unique identifier, but as we’ve seen that’s not always the case. It can happen that the desired quantity is produced in different timeframes and given the urgency it is better to start shipping the goods instead of waiting for the complete materials. Another situation may arise if the Purchase Order is unique for the vendor, but he has multiple production facilities and the goods cannot be consolidated in one shipment before being loaded on the vessel. In these case multiple approval tables will contain the same PO and will be individually recognised from the weight or volume of the freight.

Ex-factory date: this is the date on which the vendor has committed to make the goods available for pick-up. It’s usually planned before the season’s start, but little variations communicated in advance can be accepted. If that’s the case, the vendor usually notifies the Logistics Team of this variation in the same mail that he attached the preliminary documents to.

As we’ll see, this date is one of the most important information of the approval process, because it’s heavily used in planning operations, as well as performance monitoring. When approved, this date cannot be changed.

Physical information of the freight: depending on the chosen mode of transport, it can consist of the weight or the volume of the goods. Both information can be found on the packing list: usually for ocean shipments the volume is the most important variable, because it implies which container has to be used, while for air shipments weight is more critical. The two container alternatives are:

- FCL (Full Container Load) implies the payment of an entire container, with a fixed price per unit. It is generally the best solution if the total volume of the shipment exceeds 20 cubic meters (20’ ft container is booked) or 32 cubic meters (40’ ft container is booked)
- LCL (Less than Container Load) implies paying a rate per cubic meter, using the space available in a container that includes other shipments too. Normally it’s the best solution for shipments with a volume of less than 20 cubic meters, but the breakeven may vary, depending on the lane

Air freight rates are provided on the basis of the chargeable weight, which coincides with the gross weight of the goods if the volume doesn’t exceed a specified coefficient (about 160 kg per cubic meter).

Mode of Transport: this variable has a great relevance, because it is tightly related to the logistics strategy of Oakley’s team. The AFA business has a bigger portfolio of shipping modes than the eyewear business. Given the lower marginality, while frames can travel by air more frequently, AFA materials are planned to go by ocean, under standard conditions. However, when there’s the need to accelerate the shipment, other means of transport can be used. We can divide the different possibilities into two broad clusters: standard shipping modes and premium ones.

- A *Standard mode of transport* is the one that was originally planned by the procurement team, at the moment of the Purchase Order creation. Normally it consists in the cheapest alternative, capable of making the goods available in store by the desired deadline. As mentioned, the most used standard mode is Ocean for the AFA business, but the category can include in some cases:
  - Truck: for some lanes Truck is preferred to Ocean for its better rates. These lanes include China to China, Mexico to US and from some European vendors to the Italian DC

    - Air-Express: Express courier services like FedEx or DHL have higher rates per kg than any other mode in the Oakley's logistics portfolio, but for small freights they can be the optimal solution, for example when minimum fees have to be paid to the global forwarder

- A *Premium mode of transport* is chosen when the planned delivery date cannot be reached using a standard mode. Given that shipments are planned retroactively, subtracting to the delivery date the logistic target of the relative ocean shipment, a premium mode has to be chosen when the Ex-Factory date is delayed. The Logistics team, depending on the transit time and the and the available alternatives for each lane, can proceed with one of the following alternatives:
    - Fast Vessel: this service is faster (and more expensive) than a traditional ocean rate, because the vessel used typically has higher sailing velocities and/or less planned stops during the voyage. The lanes that they cover have their origins mostly located in south America, while the usual destination is the US distribution centre of Atlanta
    - Rail: shipments by rail are only available from China to Italy at the moment, which is one of the most important ones in terms of total volumes shipped. They offer shorter transit times (ca. 40%) and charge consequently more. The price is set only for Full containers, so the possibility loses sense for LCL ocean shipments to accelerate
    - Sea-Air: this service consists in a partial ocean shipment, usually for the first part of the voyage, followed by an air shipment for the final part. The two available options, in terms of destinations, are US and Italy, while the origin possibilities are broader but don't include all the Oakley's vendors. The possible airports of origin are Singapore and Dubai, so rates are provided with double values for each lane, depending on the origin airport

- Air: air shipments are the most expensive, but also the ones that guarantee the shortest transit times. Oakley's Logistics Team has updated rates for all the covered lanes, so Air is always available as an alternative

It's important to mention that no single mode is Standard or Premium per se, but it depends on the fact that it was chosen in the planning phase or as an acceleration measure. For example, both samples shipments (which take place one year before their relative season) and special capsule collections are entirely planned with Air shipments, that in this case can be seen as standard modes of transport.

Incoterm for the shipment: as the contractual terms are negotiated before the season logistics planning, these terms are fixed and known by the vendor in advance. The two most common incoterms in the AFA logistics process are:

- EXW (Ex Works): in this case the vendor has to make the goods available for pick-up at the manufacturing facility. The client (or its forwarder) needs to load the freight directly at the producer's factory, who after that moment loses any responsibility over the transported materials
- FOB (Free On Board): in this case the vendor is contractually obligated to transport the goods to the origin port (or airport for air shipments). Only after that its responsibility over the goods ends

It's important to mention them to the Forwarder, because they impact the pick-up location and the readiness date of the materials. For example, if the vendor declares under FOB terms that the Ex-Factory date will be in seven days, he must make the goods available for the forwarder in seven days in the specified location, not at the manufacturing facility. If the goods are produced within seven days but the materials reach the loading port on the 8th day, the vendor is considered on delay and could incur in penalties.

The designated forwarder: the denomination must be written in the table, but a referent has to also be put in copy in the e-mail communication for future arrangements with the vendor. Only in case of Air-Express mode this field can be left blank, because the vendor will autonomously arrange the shipment with the courier he chooses.

The final destination: this field can be filled with one of the six DC of Luxottica. In case of shipments going directly to the final customer (called *Direct Shipments*) the precise address has to be written.

The IN-DC delivery date: the date, by which the goods have to reach the final specified destination. Therefore, also the last mile voyage has to be added to the transit and navigation time. This date is calculated by the Logistics Team, adding the target provided by the forwarder in the RFQ (Request for Quotation) to the declared Ex-Factory date.

The following communications between the vendor and the forwarder are usually kept offline, or don't include the Logistics Team, except if issues arise. The Forwarder will arrange the pick-up of the goods at the vendor's factory (in case of EXW terms) or at the loading port (in case of FOB terms) on the planned date. Global forwarders have local offices in many countries, but for obvious reasons not all lanes are covered by a local proprietary branch. Therefore, in many cases they'll use external local agents, who will be employed to arrange the pick-up for them. These local agents never communicate with the Logistics Team, making this part of the process extremely opaque and characterized by scarce visibility for all the stakeholders.

Once available, the forwarder will then provide the logistics team a sailing schedule, answering to the same mail thread mentioned before. The sailing schedule must include the Estimated Time of Departure of the Vessel and the Estimated Time of Arrival at the destination port.

The Logistics Team has to give a final approval to the proposed schedule, checking that the desired delivery date is respected; given that no estimate of the last mile transit time is provided, the calculations can be made only on past last mile performances for the same destination.

Once the sailing schedule is approved, the forwarder (or the local agent) is responsible for delivering the goods as planned. He will pick-up the goods, together with the commercial invoice, on the Ex-Factory date. It's important to stress that the Actual Ex-Factory date can be considered equal to the planned one (and the vendor consequently on time) only when the forwarder has the full ability to proceed with the shipment; this means that delays in the creation of the commercial documentation, even when the physical goods have been made available on time, can cause the delay of the shipment, with the responsibility being completely given to the vendor.

It was worth specifying this type of situation because it represents one of the most common disputes that can arise in the international logistics sector, and its causes can be found in the lack of transparency and visibility along the chain. While materials discrepancies or errors can be easily detected and the vendor can be blamed, for documentation issues it is not always simple to understand who was responsible for the delays at origin, whether the vendor itself or the freight forwarder. In many occasions they'll both blame the other and it can be extremely difficult to deep dive in the situation, especially if the process takes place in a country where neither Luxottica nor the freight forwarder have local offices.

Once the goods have been picked up, the forwarder brings them to the origin port's loading area, where the necessary port and custom operations can be completed before loading the container on the vessel. The port operator, together with the goods, asks for the commercial documentation, including the Bill of Lading which give him temporary possession of the cargo. He then transports it to a specified area where export customs clearance processes take place. Before being loaded on the ship, the container is weighed and its mass (VGM, or Verified Gross Mass) digitally or physically saved for future checks at destination.

Given that the considered case consists of an FCL, during the voyage it won't be opened, and the goods won't be re-organized in other containers.

However, changes of vessel are possible, and are one of the main causes of loss of visibility from the client, that sometimes are not informed of the name of the new ship and therefore cannot locate their cargo until it's arrived at destination.

At the arrival port, the container is inspected immediately after being unloaded: its actual VGM is checked against the one measured before sailing, and the operators confirm that the seal has not been compromised, implying that nobody has opened the container during the voyage. These two confirmations act as legal proof that the cargo has not been compromised and contains what is stated in the original Bill of Lading.

The customs clearance process is usually done by the global forwarder but can be delegated to external companies if needed or better fees are offered. The procedure requires all the aforementioned commercial documents, plus some additional certificates, like EUR1 or FORM-A, that allow for tax reduction for some special lanes and products' business families. These documents, like the Bill of Lading, have to be sent in original copy via express courier to the clearance services providers. This is another inefficient operation that can cause useless delays and therefore demurrages costs at the destination port.

After the customs processes are completed, the cargo is handed over by the port operator to the last mile courier (usually the global forwarder or its local shipper) for the transportation to the final destination. The last mile operator needs to book an appointment with the Distribution Centre, declaring the date and time of arrival, together with relevant identification data of the vehicle that makes the recognition of it possible at the DC entrance.

Once the freight has been successfully delivered, the Proof of Delivery (PoD) is signed by the consignee and the last mile operator will send it in original form to the Global Forwarder. With this document, the Global Forwarder is allowed to invoice the relative costs to the Logistics Team, using the agreed rates and incoterms.

Chapter 5 - Case Study: the Blockchain Solution

5.1 The Solution Proposal

What follows will be a detailed example of how the same process outlined in the previous chapter can be re-thought using the latest advancements and platforms available in the field of blockchain and distributed ledger technologies. It is the result of a deep analysis of the main pilot projects of the moment, including the ones mentioned in chapter 3.

Practicality has been one of the key objectives of this formulation: it means that only technologies available at the time of writing have been taken into consideration, as if the solution would have to be immediately implemented in the company. Although the blockchain space is in constant evolution and innovations like the aforementioned payment channels and sidechains are showing a way of overcoming some of the remaining obstacles to broad adoption, only proved and functioning technologies will be implemented.

The chosen software architecture is made of public and open source resources for the most part, for a double reason: on the first hand, open source and decentralized projects, not commercially related to a single company or associations, are the backbone of the entire blockchain movement and philosophy. All the best projects in the field are generally open to a broad community of developers that in exchange provide a constant and valuable source of new ideas, testing and case study to improve upon.

On the second hand, public projects normally drive down implementation costs and lead times and are less subject to expensive maintenance.

5.1.1 The Blockchain choice

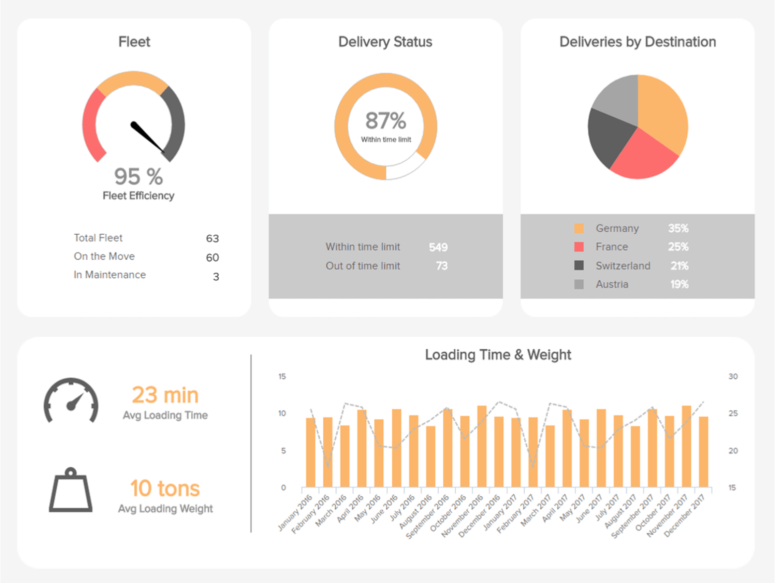
The solution will be based on the public Ethereum Blockchain. As previously explained, Ethereum is currently the most reliable blockchain on top of which smart contracts can be easily written and updated. Even though no code snippets will be showed in this explanation, it has been estimated that the entire contracts needed for this application can be written in some hundred lines of Solidity, the native programming language used in this platform. Its track record of security and continuous testing makes it the most suitable choice for such an application pilot.

The development ecosystem of Ethereum gives another important advantage, consisting in the availability of *oracles* that can generate the input data needed for some of the features described in the pilot. An oracle is a trustless and distributed source of external data, like gps position, weather sensors or simply the exact time, that can be used by a smart contract to execute its logic. Oracles were born to guarantee the same security obtained through a smart contract also to its inputs, which are inherently connected to the real world and therefore at risk of being compromised.

The limitations of public blockchains, like low throughput rate and relatively high transactions fees won't impact significantly the financial advantages of the solution proposed, given that the current process imposes to the company costs that are much higher.

5.1.2 The platform

The proposed solution will include a web-based interface, directly linked to the Ethereum blockchain. All the data will be retrieved from the blockchain but presented in a user-friendlier way to the end consumer, for a simpler experience. Figure 5.1 shows a neutral and theoretical example of how a similar platform may look like:



Total Fleet	63
On the Move	60
In Maintenance	3

Within time limit	549
Out of time limit	73

🟧	Germany	35%
🟥	France	25%
■	Switzerland	21%
▨	Austria	19%

Figure 5.1: Example of a web-based interface for the platform.

The details of the interface design won't be discussed in this work, since these choices won't influence the impact of Blockchain technology in the actual logistics process of the company. Its development could be done in any modern programming language.

However, it's worth underlining that the platform will act only as an interface, a tool to interact with the Ethereum network in a simple way. Every transaction, status modification or smart contract execution could be seen as well using any available blockchain explorer (like EtherScan.io), even though its data would be encrypted.

For any sensitive operation, like querying a secret piece of data or giving a formal approval, the platform will ask the user to sign the request with its hardware device, thus ensuring that he is authorized to do so.

5.1.3 Hardware verification

Every actor will be identified by a public address, whose level of secrecy will be decided by the network leader, in this case Luxottica. The leader can also manage who knows the identity of each address, reaching the desired level of openness between the chain members. Just as we've seen in the technical explanation of the Bitcoin protocol, key pairs of private and public addresses are unique, and verification can be made by anyone, without ever seeing the private key of the other members. If, for instance, an address tied to a specified port operator signs a message stating that he's in possession of the goods, we can be sure that the sender was not anyone else except the proprietary of the private key, with the same security we have in a Bitcoin transaction.

Every actor will use its unique and proprietary hardware wallet to sign the transactions. If needed for multiple geographical regions, the authorization will be given to multiple addresses per member, but the unicity of each address will be maintained. This infrastructure gives to the entire network a certification that the status of the goods is updated only by the person that, in that precise moment, has the authorization to do so.

The proposed hardware is the *Ledger Nano S*, one of the most common hardware wallets currently available. The company could be able to design and produce its own wallet product, but this choice derives from the tendency to prefer open source and sufficiently tested solution over private initiatives. Such products' cost is extremely low (about 100$) but their efficacy and reliability has been enforced by several years of activity without any breach. An example is shown in Figure 5.2.

Figure 5.2: Ledger nano S, the most adopted hardware Ethereum wallet

5.1.4 Documents' tokenization and decentralized storage

It's worth explaining in greater detail what happens when the phrase "hashing and storing a document" is used, given that it will appear many times in the proposed solution. Creating a unique identifier for a physical document is one of the key steps to ensure the success of a blockchain application. As we've seen, most public blockchains have never been hacked or compromised for many years, and therefore their security can be assumed with a reliable degree of certainty. However, if the management of the data can be processed with absolute security and immutability, the link between the physical element (a document, the goods shipped and so on) and the digital assets on the blockchain is the critical factor that determines the success or the failure of any blockchain solution for supply chain management.

Turning a document into its digital fingerprint is quite easy and many options were available well before blockchain. For this solution we'll assume to use the MD5 hashing algorithm (https://md5file.com/calculator) that accepts files of any type and calculates the hash in text form. As for every hashing function, it is worth remembering that changes to every single byte of the file would result in a completely different hash, and from the hash is impossible to retrieve the original document.

Once the file is properly hashed, though, storing it becomes the key problem: blockchains are inefficient for storage, given the maximum block size and the high associated transaction costs.

The most adopted solution used in the market is IPFS (the *Inter-Planetary File System),* which we've encountered in the previous chapter. This protocol was born with the aim of revolutionizing the way content is stored and retrieved on the web. It's designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. Today's internet mostly works in a centralized fashion: websites are powered by central servers that ensure the maximum resources (storage and bandwidth) at the minimum price. This structure, as for any centralized network, can be affected by corruption, censorship or malicious attacks, that can alter the contents stored or worsen the service they provide.

The solution proposed by IPFS changes the way content is retrieved from any web service. The majority of modern websites use a paradigm called *location-based addressing*: that means that every user specifies, with his computer, where the content he wants to see is located, in the form of a website link or a domain name. If, for any reason, the location you provide to your browser isn't accessible, you won't get the file. However, even if the servers are currently down, there's a high possibility that other users have already downloaded the same file you're looking for, but in order to retrieve it you'd have to know its precise location.

IPFS changes the search model to a *content-based addressing*: in simple terms, instead of stating where to find a resource, you search directly the resource you're looking for. In order to recognize the precise file, every media is hashed in the IPFS network, therefore being linked to a unique identification code. The hashing algorithm ensures that each file is completely mapped into its code. In this way, when a peer sends it to you, it's easy to check that the same file has not been tampered, because any minimal change on it would result in a different resulting hash.

Another advantage of this structure is that identical copies of a file can be recognized (they will have the same exact hash) and therefore each node will only keep one copy of it, saving resources and gaining efficiency. The atomic element of the IPFS network is called IPFS object. Figure 5.3 shows an example of this data structure:

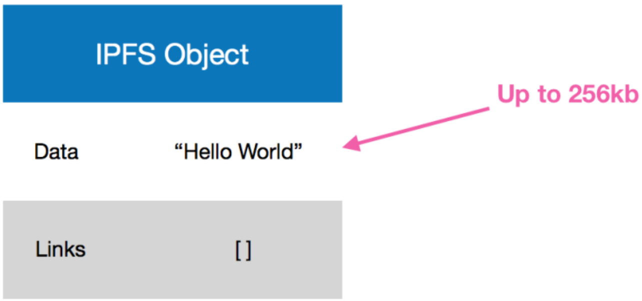


Figure 5.3: an example of IPFS Object, containing a Data field and a Link field.

Such an object can contain up to 256 kb of data and links to other IPFS objects. For any media file greater than that (like images or videos), the file is split up in different 256bk objects, and an additional empty IPFS object will be created with no data in it but containing the links to locate all the pieces needed to reconstruct the original file in order. The same linking property can be used to store files on the network in a predetermined structure, for example made of folders and subfolders. It will be sufficient to create as many additional empty objects as needed to state the desired file paths, as explained in Figure 5.4:

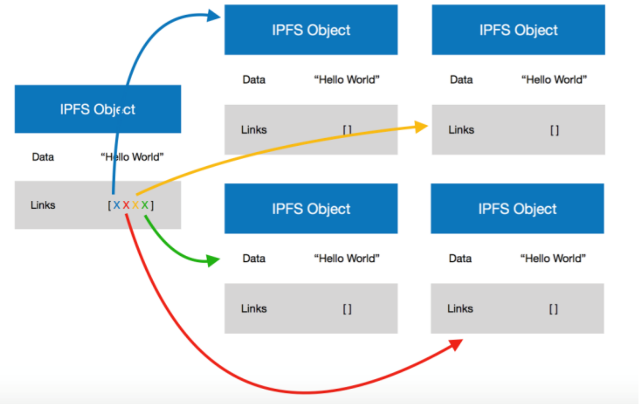


Figure 5.4: Linking feature of IPFS Data Objects.

This objectification of files tied to a unique fingerprint makes also versioning possible. In fact, changing or updating a file will cause the hash to change, generating a second file distinct from the first one. A special object type called "Commit" can be used to store, together with the hash, also the parent file to which this media is a subsequent version.

The main risk for this solution is to lose track of a file, if all the nodes having it suddenly disconnect themselves from the network. A possible solution could be to always keep a copy of each file in a proprietary storage, in order to access it in the remote possibility that for some reason none of the encrypted copies are available on the IPFS platform.

A second solution currently in implementation is the incentivization of nodes to store and keep online the files they have, through a cryptocurrency called Filecoin. It was proposed by the same group that developed IPFS, with the aim of improving the reliability of the network by giving people a monetary incentive to stay connected, just as Proof of Work for the Bitcoin protocol.

5.1.5 Process proposal

Now let's deep dive in the actual process redesign. All the steps described in the As-Is chapter will be revisited, introducing the benefits that blockchain technology could bring using the chosen information and hardware architecture.

The figure below (Fugure 5.5) summarizes the new process structure. It is divided into the most critical milestones: the Shipment's approval, the Pick-up, the loading and unloading of the FCL container, the Customs Clearance activities and the Proof of Delivery at the final destination. All the actors will have restricted authorizations to write on the blockchain and/or read data from it for each waypoint.

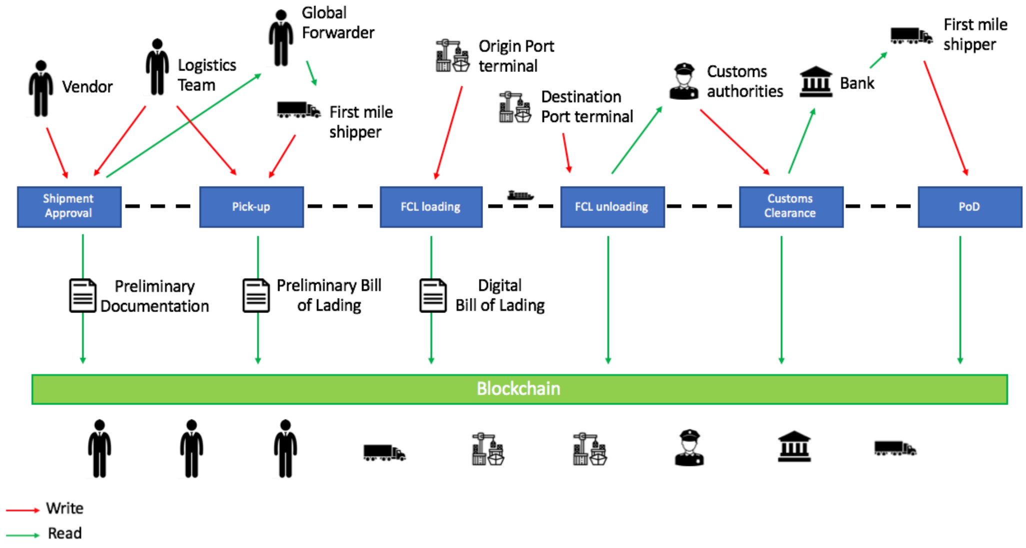


Figure 5.5: structure of the new Blockchain-based process.

Let’s analyze each step:

Before the pick-up: the vendor uploads the preliminary packing list that will be hashed and stored, tied to its digital fingerprint and saved on the IPFS network. The choice of a standard PDF or excel format would help recreating the same file knowing all the info that were contained, but it is not mandatory. The document’s hashing would work even with a .jpeg scansion of the hand-made document.

The vendor will have the possibility to change the file, but no past data can be deleted or altered. If multiple versions are uploaded, for instance because more precise data of the shipment become available over time, the logistics team will be able to see the complete changes history and confirm if the definitive file has been correctly sent before the hard deadline, simplifying dispute resolution.

Within 6000 blocks (approximately 24 hours) from the original upload of the file, the Logistics Team has to confirm its correctness, signing the document with its private key. The criteria for correct packing lists will be only numeric, like the number of SKUs for each material and size, in order to prevent useless and time expensive disputes.

The Logistics Team will then have 5 days (about 30’000 blocks) to publish the approval table on the platform, which must contain all the relevant data for an effective arrangement of the shipment, including:

- The authorized Ex-Factory date
- The chosen mode of transport
- The in-DC date, which cannot be closer from the Ex-Factory date by more than the agreed transit time
- The Incoterm

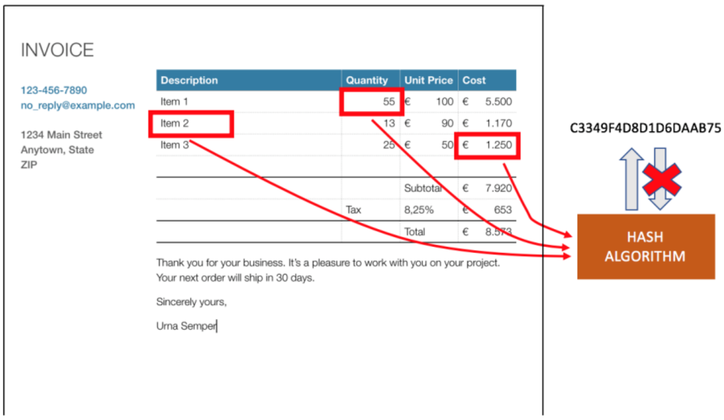
The platform will automatically compute the optimal parameters, at least for some of them, and prompt them as proposals, that the Logistics Team can accept or overwrite. As like for every other important document in the process, the approval table will be hashed and stored on the IPFS network, as well as on the platform.

The vendor uploads the invoice and the tracking number of the shipment, no later than the day after the agreed Ex-Factory date (the 24 hours delay is granted in case the tracking number is provided to the vendor on the day of the pick-up). These two items will be used to generate what will be called a *preliminary Bill of Lading*, that will act as the confirmation of ownership of the goods before the actual Bill of Lading is issued. This preliminary Bill of Lading is a hash of some of the contents of the commercial invoice and/or the packing list, whose generation will be further analyzed in the next paragraph.

From the pick-up to the port: as we've covered in the description of the AS-IS process, many actors can be involved during the pick-up of the goods and the actual loading of the same goods on the vessel. Especially in remote origin countries, where the freight forwarder doesn't have a local office or a proprietary shipper fleet, he will use local agents to organize the operations, who could also outsource the actual job to independent shippers they have contractual agreements with.

Therefore, it's important that the Logistics Team and all the other interested parties maintain a clear visibility on who is taking care of the goods at any moment, plus the exact location (as more as possible) of the same cargo. At the same time, local shippers cannot have the same access to the history of the goods, for security reasons.

The key objective is to make every actor in this phase able to update the status of the shipment, without seeing the past history of the same shipment. This can be done in the following way: the platform will arbitrarily choose some variables between the one included in the commercial invoice and hash them together to generate a unique code (the preliminary Bill of Lading mentioned above) that will represent the goods on the blockchain. These variables can be anything, from the total volume of the freight to the third item code on the materials list. In Figure 5.6 we can see how the algorithm works.


INVOICE

123-456-7890
no_reply@example.com

1234 Main Street
Anytown, State
ZIP

Description	Quantity	Unit Price	Cost
Item 1	55	€ 100	€ 5.500
Item 2	13	€ 90	€ 1.170
Item 3	25	€ 50	€ 1.250
		Subtotal	€ 7.920
	Tax	8,25%	€ 653
		Total	€ 8.573

Thank you for your business. It's a pleasure to work with you on your project.
Your next order will ship in 30 days.

Sincerely yours,

Urna Semper

Figure 5.6: functioning of the preliminary Bill of Lading creation.

Each actor, when receiving the goods, will be prompted to fill a form with a random subset of the invoice data, containing also the identification ones, and will therefore generate the same hash value that is located on the blockchain. The status of the goods will be updated, stating that the possession of the goods has been given to the new address. The smart contract will authorize this update of the shipment's status as valid and change the goods status accordingly. All data recorded on the blockchain will be encrypted, so that even the operator won't be able to recognize his update, between all the transaction included in the same block.

It's worth underlining that, even if the single parties can see their transaction updating the shipment's status, nobody in the chain, if unauthorized, can look at the complete history of the shipment. However, at the same time, everybody that physically possess the goods (or knows the data of the commercial invoice) will have the implicit right to update its status, based on its personal address' authorizations.

The agent will take care of the first mile transit, delivering the goods to the port operators at the designated port. This change of ownership will be also documented as a status change tied to the preliminary Bill of Lading.

At this point the actual Bill of Lading will be issued by the shipper and sent to the Vendor, who will proceed in creating a digital tokenized version of it, similar to the one we've seen in the CargoX solution. A digital fingerprint of the document will be issued, comprising all its information in detail, so that a minimal change on every aspect of it will make the copy illicit. The resulting entity on the Blockchain will be an ERC20 token that the Exporter can send to the smart contract in charge of the operational processes. The same contract will check that the goods are correctly loaded on the vessel, and that all the required anticipated payments (if expected) have been correctly submitted. If all the conditions are met, the smart contract will forward the token to the logistics team, effectively making it the new unique owner of the digital Bill of Lading, and of the goods as a consequence. In Figure 5.7 a simple example of Bill of Lading tokenization and decentralized storage is showed.

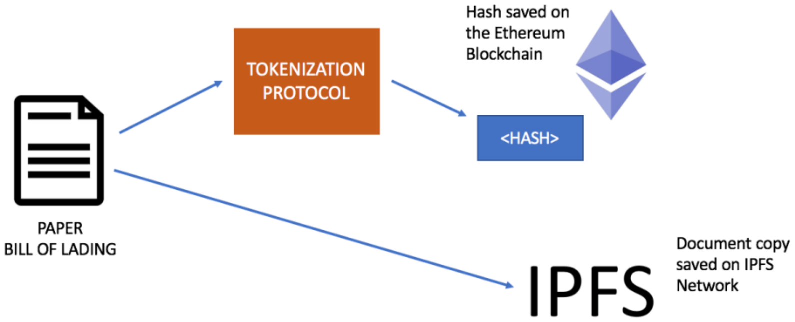


Figure 5.7: tokenization and storage of the actual Bill of Lading.

The voyage: a set of sensors could be installed on the container, updating its position, temperature and humidity variations on the blockchain, in a periodic fashion. Each one of these sensors will be tied to a unique key pair that makes it recognizable on the blockchain, ensuring its authorization. In this way, the position of the goods can be monitored at any time and unexpected events like navigation delays can be anticipated, giving the logistics team a chance of acting on them.

Customs Clearance operations: as we've anticipated, customs declarations involve a frequent and inefficient exchange of information between all kinds of operational and government actors. Communication is extremely redundant and therefore delays soar as a consequence. Custom operations require in essence no manipulation of the data, but only a disclosure of it. In particular, what the authorities usually want to see is:

- The commercial value of the goods, as stated in the commercial invoice
- A detailed description of what the contents of the container is, as written on the packing list
- Information about the logistic process the container has been subjected to. For this type of request the Bill of Lading is usually enough

The proposed platform will make all the previously mentioned data available at no additional costs, paired with relative timestamping and versioning details. If any data has been changed along the goods transit time, customs operators will be able to see if the modification was licit or deserves deeper analysis.

Data won't be disclosed only at the moment of the declaration, but instead could be accessed from the moment it was appended on the blockchain for the first time. This feature allows for increased automation of the clearance inspection algorithms, that could know in advance which cargos retain the more risk, depending on many factors like the origin loading port or the history of the company responsible for the shipment.

Needless to say, the solution is proposed on the important hypothesis that government authorities would trust the Blockchain ledger as a reliable source of data, capable of making the information untampered and completely adherent to reality. For this to become a reality, an international and shared effort must be incentivized in the coming future.

Last mile transportation and final delivery: when the goods are successfully cleared after the customs inspections, the operator responsible for the last mile transportation will pick them up from the port. The importer will use the Bill of Lading to prove its possession of the goods, which has been previously sent to him on the Ethereum blockchain by the exporter. From this point, the digital Bill of Landing is not needed anymore and the pick-up can be followed simply by a status update on the preliminary Bill of Lading, created at the moment of the commercial invoice generation.

The operator would only need to type into the platform the asked data, available on the invoice he receives together with the goods, and a status update will be sent to the secret hash representing the shipment, that only Luxottica and its authorized partners know. Just as in all the other waypoints, when the goods change hands, the confirmation of identity of the operator will be derived by the address responsible for signing the transaction, that will be uniquely tied to its hardware device.

At the final destination, after the appointment has been booked, the receiver (one of the company's DC employee) will send a timestamped confirmation that the goods, represented by their hash, have successfully arrived, checking that the quantities written on the invoice exactly match the physical ones, and no damage has been made to the goods. This final confirmation, authorized by one of Luxottica's address which are mapped into the smart contract's code, will definitively close the shipment and freeze its hash, which will no longer accept status updates.

The completion of the physical shipment will trigger the smart contract responsible for the financial payments, enabling the vendor of proceeding with the invoicing of the materials and the request of the funds, as negotiated for the Purchase Order.

5.2 KPIs definition

The aim of this paragraph will be to present a qualitative evaluation of the solution proposed, from a financial, operative and information point of view. In the first section nine KPIs will be defined and described, which were structured to model the company's requests in terms of financial, informational and operational performance. Thereafter, an estimation of the improvement or worsening caused by the blockchain solution for each dimension will be given, adequately grounded by detailed explanations.

We've already covered the general advantages of blockchain technology, as a solution for supply chain implementations, so in this paragraph its efficacy will be measured relatively to indicators that are the most critical for the company, not directly tied to inherent values of the technology like trustfulness or decentralization.

It is worth underlining that, since the pilot has not been implemented yet, evaluations are purely theoretical, even though they were formulated after intensive technological research and comparison with other active pilot projects in the field.

As anticipated, KPIs will be divided into the three main areas that characterize an international logistic process: the operative flow, the financial flow and the information flow. For the operative flow, the chosen indicators are the *delay at departure*, the *time spent in customs clearance processes* and the *forwarder on time percentage*. For the financial flow, the indicators are the *overall cost of the shipment's documentation* (that includes all the arrangement and services costs needed from the Purchase Order creation to the final destination of the goods), the *documentation errors occurred* and the *easiness of dispute resolution*. Finally, for the information flow the indicators are the *overall security of information shared*, the *speed of information access* and the *flexibility of the platform*. Below a brief definition of each measure:

- *Delay at departure***:** it can be defined as the time interval between the pick-up of the goods and the actual departure of the vessel. It's assumed that no delays happen at the origin location, so that the pickup date exactly corresponds to the Ex-Factory date of the PO. The number of days needed to reach the origin port is also subtracted, because it can vary based on the distance between the port and the manufacturer's facility. This delay is usually the greatest one of the entire shipment. Freight forwarders need to find the cheapest ships, in order to increase their marginality since the price they charge Luxottica is fixed. This can cause the shipment's departure to delay, sometimes even for several days. These effects are considered in the target transit times used for the planning activity, calculated with an adequate buffer. However, minimizing the impact of this lead time increase would benefit both the business and the logistics departments.

- *Customs clearance lead time:* Customs operations pose the highest risk on an international shipment's lead time. They're made only for a fraction of the incoming containers, on a semi-random basis. Although some lanes are more actively monitored than others for security reasons, it's impossible to predict how intensive and time consuming the operations will be at the time of departure or planning of the shipment. This unknown variable creates the need for other lead time buffers that can generate inefficiencies and decrease the go-to-market speed of the business. Moreover, in the event of not passing the controls, transit times can significantly grow, and costs would soar as a consequence, for example in the form of demurrages fees at the destination port.

- *Forwarder on time percentage:* it is the punctuality of the freight forwarder, or the shipper in general (for Air-Express shipments, arranged without a freight forwarder, it will be the performance of the express courier). The indicator is measured in terms of the percentage of pieces, scheduled in a given period (usually a season) that arrive on a date equal or prior to the IN-DC Date. It is the most important indicator used also by the top management to assess how the logistics is performing, compared to the yearly targets. As anticipated, we'll be considering the *net* value, measured relatively to the exact delivery date, but other two gross variants exist: the on time *plus one day* and the on time *plus one week*.

- *Overall costs of the shipment's documentation:* we'll consider for this indicator only the total costs that can be directly tied to the single shipment, so development and implementation costs of the platform will be ignored. Given that no detailed design has been formulated over the platform's software features or graphical characteristics, it is assumed that its cost would be equal to the actual price paid for the vendor management product currently in use. Essentially the considered fees will be related to the document's creation and management, plus the costs that would have to be sustained for the same level of shipments monitoring that blockchain can offer.

- *Documentation errors:* human mistakes in the shipment's documentation can be significantly expensive, both in terms of direct costs in re-issuing the documentation and in terms of lead times increase. Moreover, these hidden costs are usually not completely anticipated nor predictable, therefore its impact can cause the budget for the rest of the financial period to reduce inadvertently.

- *Easiness of dispute resolution:* In a highly manual and not automated supply chain, as the international logistics one, disputes and misunderstandings happen quite often. As mentioned in the previous chapter, the most common arise in the pick-up phase, usually as a consequence of a misinterpreting of the incoterms and the relative pick-up location or a delay of the freight forwarder. Most of the times each one of the two parties will blame the other for the responsibility, in order not to incur in penalties, and it is hard for Luxottica to understand what happened, given the geographical distance and the scarce monitoring of the first mile operations.

- *Security of information shared:* it can be qualitatively measured as the risk of a breach of information by an external attacker. This indicator is critical for an evaluation of the solution, because secrecy over Luxottica's vendors or its contractual agreements with the forwarders is part of the strategic advantage of the company and its leading position in the market as a consequence.

- *Speed of information access:* it is considered as the time needed to retrieve the information from the platform. The solution has to be responsive to match the request of a multinational reality like Luxottica. Even though, as covered in the previous chapters, blockchain technology sees in latency one of the current obstacles to adoption, its implementation has to at least reach a sufficient level for it to be taken into consideration.

- *Flexibility of the platform:* not only the AFA business unit, but the entire company is in constant growth and renovation. Therefore, its information systems and protocols must be designed in order to match the same level of flexibility and reactiveness in the event of a change in the supply chain processes or the actors' responsibilities. At the same time, small improvements and fixes will be necessary on a periodic basis, and velocity must be an indicator of the value of the proposed solution.

5.3 KPI evaluation

What follows is a qualitative but detailed analysis of the impact that the proposed solution would have on the existing logistics process. It's important to stress one more time that, since the project has not been implemented by Luxottica yet, all the conclusions are the result of a collaborative but theoretical analysis. Every indicator previously defined will be tested against the new paradigm and its new values compared with the previous thresholds. In this way the effectiveness of such a case study can be formulated based on the aspects Luxottica's management cares the most about.

Data sources, when needed, will be always declared, and if assumptions will be made they'll be motivated in an exhaustive way. For all the conclusions, present data and capabilities of the technology will be taken into considerations, underlining the fact that the aim of this work is to show how blockchain technology could impact the supply chain industry of the present, not a distant and uncertain future.

5.3.1 Delays at departure

As we've seen in the previous introduction, delays occurred from the readiness date of the materials, which is equal to the pick-up date if no complications arise, to the actual departure date of the vessel can vary and are one of the main sources of uncertainty about the total transit time a shipment will have.

During the internship experience, where shipments were monitored from the moment in which the vendor sent the preliminary documents, this delay was constantly analyzed in order to make sure that the freight forwarder wasn't accumulating delay in the first steps of the shipment, something that could cause the entire service performance to sink under the minimum level.

Unfortunately, Luxottica cannot impact the speed with which the forwarder books the ship and loads the container. As long as they don't exceed the target transit time negotiated and the service level is sufficient, no pressure can be made to the partner. Shipments planning takes this effect into considerations, in the form of a security coefficient applied to the targets that the logistics department communicates to the Planning & Procurement team in the moment of the PO creation. However, losing days before the loading of the goods erodes the margin that the network has to reach the destination on time, putting pressure on the unloading, customs and inbound processes that cannot tolerate any delay or may have to be accelerated paying a premium price.

Given that the responsibility of this delay is minimally influenced by the company, an innovation in its information systems won't have much impact on the indicator. The blockchain solution proposed will increase transparency and reliability over the communicated dates and the occurred events but will have little effect over the minimization of this lead time.

On the other side it is reasonable to assume that the distributed and open structure of the platform, giving access to the key waypoints to all the interested parties, should improve the ability of the freight forwarder to monitor the approval of the shipment since the preliminary packing list is issued by the vendor. For obvious security reasons, data of the vendor or the planned shipment cannot be disclosed with the forwarder until the Logistics Team formally approves it and designates the same forwarder as official partner for the transportation. However, some critical data could be made public inside the network, such as an approximate estimate of the goods' total weight and volume, as well as the products' business family (if they are socks or bags for example). Every forwarding partner would see these new shipments proposal coming, without having access to the detailed information, and could consequently planning a hypothetical shipment in advance, opportunely weighing its benefits and risks.

For these reasons, we can assume that the blockchain solution would generally improve the ability of Luxottica of reducing the delays at departure, but not in a significant nor robust way.

5.3.2 Customs clearance lead time

The process of import customs clearance of the goods is done by authorities which are obviously independent from Luxottica and are generally facilitated by the global forwarder or some other external party. Even though the company is not directly involved in the process, the greatest impact on the total duration of the customs activities can be imputed to the availability of the needed documents, which have to match to the actual freight specifications.

As we've covered in the solution proposal and in some of the mentioned case studies of the previous chapter, customs operators would benefit from a blockchain infrastructure because the ledger would act as a source of reliable documentation whose history is clearly visible and accessible from the moment the documents are first issued. Verifying the correctness of a certificate by its hash, which is cryptographically proven to be unique, could take a fraction of the time needed today for the notarization and audit of the same file. In practical terms, blockchain technology could be embedded into Customs' practices through a common platform which would embrace trade-related commercial entities (Okazaki, 2018).

From a more ideological point of view, making the customs authorities part of the permissionless (in this case) or permissioned blockchain solution means investing in a transparent and compliant attitude not only towards the other peers, but also the government and fiscal institutions.

For the cited reasons, the impact of blockchain on the customs clearance lead times can be rated as significant, promoting a faster and leaner process compared to the present one.

5.3.3 Forwarder on time percentage

As introduced, this parameter is one of the most important and observed indicators in the entire logistics department of Luxottica. The percentage of shipment that arrive on time, expressed in number of pieces in a given timeframe, is the final result of all the efforts made from the entire logistics, as well as an indirect indicator of the success of the planning and sourcing activities.

Given this focused attention, it is easily understandable that the current values are quite high, reaching almost 100% in many cases. Therefore, any innovation in the information and data structure of the process cannot fuel a substantial improvement on it.

What can be positively impacted is the consistency of it, which now sometimes suffers from sporadic events and unexpected delays. Blockchain technology, especially through smart contracts, can incentivize the respect of a common set of rules and benchmarks, assigning automatic bonuses or penalties if they are reached or missed. Such a bonus structure would allow payments (even partial) to be immediately released if the conditions are met, and its logic can be trusted by the entire network thanks to the underlying cryptography and the use of decentralized oracles for external data inputs.

Such incentives can be implemented also using a traditional information system, but blockchain ensures the predictability and trustfulness of the agreement in a way that was not possible before.

Given the premises, we can state that blockchain's impact would be surely beneficial to the general improvement of the indicator, both from an average point of view and from a peak one, limiting the extreme situations by enforcing a reliable set of incentives for the forwarder. However, the influence cannot be proportionally positive as the previous one, given the already good results obtained by Luxottica's team.

5.3.4 Overall costs of the shipment

As we've anticipated in the introduction of some of the case studies, documentation costs for an international shipment can add up to 15-20% of the entire container's cost. The main sources of value paid are:

- The issuance and manipulation (including shipment) of paper documents which to this day retain high importance, like the Bill of Lading or the Forms needed for tax reduction
- The redundancy of communications between parties, consequence of the "push logic" from which documents are sent multiple times to the interested peers in order to prevent delays in notifications
- The general premium price paid, both to information systems and to trusted intermediaries, to minimize information asymmetries between the actors

Efficacy is preferred over efficiency when it comes to logistics communications, at least if the marginalities allow for it. Blockchain technology will positively impact all of the three main causes of documentation costs:

- With an effective protocol for documents digitization, tokenization and decentralized storage, the need for paper can be minimized. We've seen that the degree of security of a tokenized asset can be significantly higher than a handwritten one, which will always be at risk of being tampered. The only variable cost (fixed costs of platform development and implementation are not taken into consideration) is the transaction fee of an Ethereum contract. Assuming a confirmation time of a few hundred blocks (equal to a few hours in the worst scenario) and a precautionary value for gas price, the total fees amount less than a US dollar. Therefore, even ignoring the security improvements of the solutions, it's clear that the financial benefits would be extremely significant.

- The theme of communications redundancy is one of the most notable drivers that characterize a process in which blockchain can be substantially beneficial. This effect comes from the fact that distributed ledger technology brings an entire new paradigm for data sharing, opposite to the one we're currently used to. In the current logistics process, data is intentionally sent to the next responsible party on the chain, and often also to other peers that have already received it in other occasions, just as a notification. These little inefficiencies seem trivial but add up to a redundancy that significantly increase the total documentation costs for a shipment. On the other hand, we've seen that blockchain normally act as a common source of truth, from which entities retrieve data if and when needed, in what can be defined as a "pull" paradigm. In this way, not only resources can be saved from the replicated sending of the same documents, but also working time of employees spent on double checking of the same files can be eliminated.

- Information asymmetries are a common defect of many information systems. The existence of separated data silos and fragmented communications differentiates the picture that the supply chain actors have. This condition poses a substantial risk of misunderstanding and the arousal of disputes that can be time consuming and expensive to resolute. The same risk is currently removed with a combination of redundant communication (that we've covered before) and the employment of a trusted central authority that certificates the validity of the data and the senders of it, in exchange of a (hefty) fee. Blockchain was born with the precise aim of removing the need for such intermediaries, first in the financial sector (with the invention of cryptocurrencies) and now in the supply chain management one. By updating the global ledger in a periodic way, completely free of charge (if no transactions are made) distributed networks essentially act as a global certification protocol, where data's provenance and chronological order can be trusted in full.

Given that blockchain technology can impact in a profound way all the three major costs areas of a shipment's documentation process, we can confidently assume that the benefits on this indicator would be substantial. It's worth remembering that transactions costs in any public blockchain are quite high, relatively to a simple data transmission in a traditional EDI system; but since this logistics application doesn't need a huge number of transactions, each corresponding to a document modification or a status update, their total sum can be considered fairly low in percentage.

5.3.5 Documentation errors

Given the high presence of manual and paper-based documentation, we've already seen that the amount of documentation errors can be quite costly for an international shipment, especially when mistakes happen to important financial documents.

Blockchain technology's capabilities are perfectly suited for preventing transmission errors, as well as intentional tampering attempt. We've seen that once a piece of information is appended to the ledger, every modification can be immediately found out and all the versions are available for further analysis, preserving the original versions of the file. Naturally, errors in the initial inputs cannot be prevented, except by making the input modules of the platform as user-friendly as possible, so that banal errors can trigger some alerts right away and possible valid alternatives immediately suggested.

We can conclude that the impact of blockchain technology in preventing documentation errors can be significant, although not at the same level of the improvements brought in the documentation overall costs.

5.3.6 Easiness of dispute resolution

The most critical and difficult disputes to take care of are the ones in which Luxottica is not a part of. This normally happens at origin, when the parties are generally the vendor and the designated forwarder, and the visibility of the process is at its lowest peak. Situations like litigation over the exact readiness date of the materials, after a delayed pick-up, are quite common: the vendor would state that the goods were available to the forwarder, but it came late, and the forwarder would claim that it wasn't true, or the documentation attached to the freight was incomplete or not accurate.

With the use of a digitized preliminary Bill of Lading that can be updated only by an actor that physically owns the goods, the company can be sure that seeing the status update on the blockchain is a proof of the correct ending of the change of hands. The parties are incentivized to transmit such update, in order to free themselves from the responsibility of a dispute that may arise. When the receiver peer confirms the data contained in the invoice, it is implicitly guaranteeing that he has received the stated material types and quantities. Therefore, if future discrepancies will appear between the quantity he received and the one that will be passed to the next actor, he would be considered responsible for the fact without the need of further expensive litigations.

As a consequence, disputes resolution will be greatly improved by the use of this proposed blockchain solution.

5.3.7 Security of information shared

Security in international logistics is really critical. Vendors contractual agreements and shipped material details can disclose a great part of a company's strategy if leaked.

Blockchain's inherent security model is well suited for such a task. It's worth remembering that the Bitcoin protocol is active since 2009, managing more than $500 billions at its peak, and never a breach has been successfully made. The same security can be assumed when we're dealing with data transmission and access in a supply chain management application. Just as like bitcoins can't be removed from one's wallet without its private key or no past transactions can be altered, documents appended to the blockchain will remain there, at least the timestamped hash of them, forever.

Moreover, if a transaction (meaning any data input or modification) has been made from an authorized address, we can be sure that he was responsible for the transmission, as long as its private key or the hardware wallet have not been leaked. Compared to the current systems, in which sometimes sensitive documents are sent by email, this is a substantial leap forward in favor of a better security and protection of the data.

5.3.8 Speed of information access

Access speed of information is obviously important in the logistics sector, like in any other business-related process management. Having the information at hand when needed can increase the overall performance as well as efficacy of the entire network.

The implementation of blockchain technology would not add any benefit to this indicator, since the lead times for accessing data on the ledger are not shorter than the modern traditional systems. Actually, even though comparable in scale, physical times to receive the retrieved data from a blockchain can be higher, due to the fact that available peers have to send the data, whereas in a centralized web structure the main server is specifically designed for achieving the maximum speed.

5.3.9 Flexibility of the platform

Every technological solution cannot be developed without the aim of being flexible when modifications or updates are going to be needed in the future. Since a detailed analysis of the platform itself would be out of the scope of this work, it will be assumed that an interface operating in a blockchain environment would be as flexible as a traditional one, since similar or equal programming languages and API call structures can be implemented.

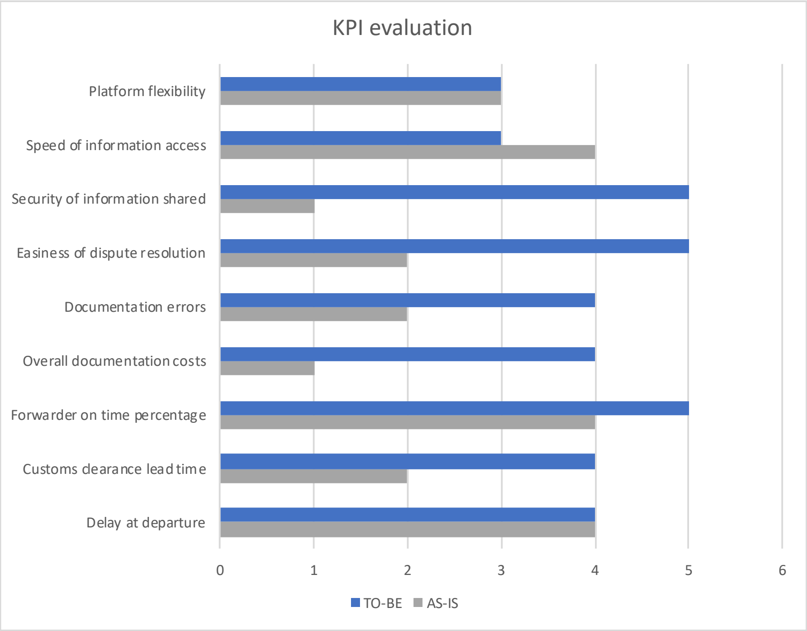
5.4 Results

Let’s summarize the evaluations made for each one of the nine key dimensions. In Table 4.1 and 4.2 we can find the grades given to every aspect, on a scale from 1 to 5, both for the AS-IS state of the process and for the proposed one (TO-BE):

Table 5.1: summary table for the dimensions evaluation, for AS-IS and TO-BE process variants.

DIMENSION	AS-IS Performance	TO-BE Performance	Delta
Delay at departure	4	4	0
Customs clearance lead time	2	4	+2
Forwarder on time percentage	4	5	+1
Overall documentation costs	1	4	+3
Documentation errors	2	4	+2
Easiness of dispute resolution	2	5	+3
Security of information shared	1	5	+4
Speed of information access	4	3	-1
Platform flexibility	3	3	0

Table 5.2: graph representation of the final evaluation of the proposed solution.



As we can see from the final results, six out of nine KPIs show an improvement over the previous situation. In two cases (regarding the delays at departure and the platform flexibility) the performance is not improved. In the first case we've explained that the ability of the forwarder to minimize the lead times between the pick-up of the goods and the departure of the ship is not under Luxottica's operational perimeter, therefore no solution could improve that KPI without an integration (at least partial) with the logistics partner.

Regarding the platform flexibility, the performance has been assumed not to change, given that details of the software and graphical interface development of the platform were out of the scope of this thesis.

In one case (speed of information access) the performance actually decreased, since blockchains have to this date inherent latencies when data is retrieved from them. Nevertheless, it is possible to assume that such latencies won't exceed the second threshold, guaranteeing a usable interface also in the event of a temporary network congestion.

The major benefits are focused on the financial flow, whose indicators would undergo the highest improvements. The reasons for this impact lay in the fact that most of the current systems and processes are designed in a redundant and inefficient way, in order to guarantee the desired level of efficacy and security. The promise of blockchain technology is to change the way we see trust in the information era, transforming the current paradigm and allowing business partners to only care about the value creation, instead of the network security and transparency infrastructure.

Conclusions

This thesis had a dual purpose. On the first hand, to give a contribution in terms of analysis in the field of blockchain technology applications for supply chain, mainly focused on the logistics sector.

On the other hand, the work aimed at giving some interesting insights to the company, which the internship and the case study was centered on. Although the improved process proposal was only theoretical, Luxottica has shown interest in the possible implementation of it and the desire to deeply elaborate on the synthetic idea.

Since literature on the subject is still limited a deeper research effort will be needed in the future, in order to better understand how this new paradigm could benefit modern supply chains and commercial human interactions.

The hope is that the entire blockchain ecosystem continues innovating and testing, attracting even more resources both in terms of smart people and investments. Many academic efforts and consortia will be needed to lay the so wanted standards, upon which blockchain adoption could flourish. Given the broad spectrum of possible applications of the technology, the hope is to see the birth of many more pilot projects, aimed at finding and/or showing the potential benefits of distributed ledgers, as well as their threats we're currently unaware of.

From a technology and infrastructure point of view, we've highlighted the most urgent limitations to be overcome. A community research effort will be needed to find and develop solutions to problems like the low throughput rate or the latency one.

As stated multiple times in the elaborate, one of the main obstacles lays in the fact that decentralized technologies require a complete mindset shift from the past, towards a more open and transparent way of managing trades and commercial relationships. Blockchain gives the technological foundations, on which leaner and more efficient information processes can be designed, but the effort must come from the users posing trust in the system. Like every other distributed system, once a critical mass of users is reached a capillary and relatively rapid adoption will probably (and hopefully) follow.

References

Adkronos (2017). Luxottica, missione e strategia del colosso degli occhiali. [online] Adnkronos. Available at: http://www.adnkronos.com/soldi/economia-/2017/01/16/luxottica-missione-strategia-del-colosso-degli-occhiali_G7AeJI-FqeKFhQyzhwH0YiP.html [Accessed 8 Sep. 2018].

Antonopoulos, A. M. (2014). "Mastering Bitcoin: Unlocking Digital Crypto-Currencies". O'Reilly Media. ISBN 978-1-4493-7404-4.

Back, A. (2002). "Hashcash - A Denial of Service Counter-Measure".

Barnes, J. G., Byrne, J. E. (1996), "Letter of Credit: 1995 Case", The Business Lawyer, Vol. 51, August, p. 1418.

Biagio, S. (2018). Piattaforma di bitcoin MtGox dichiara bancarotta. Persi 345 milioni di euro. [online] Il Sole 24 ORE. Available at: http://www.ilsole24ore.com/art/finanza-e-mercati/2014-02-28/piattaforma-bitcoin-mtgox-dichiara-bancarotta-persi-345-milioni-euro-160351.shtml?uuid=ABXu8tz&refresh_ce=1 [Accessed 12 May 2018].

Bitnodes.earn.com. (2018). Global Bitcoin nodes distribution. [online] Available at: https://bitnodes.earn.com/ [Accessed 10 Apr. 2018].

Brunetti, G. and Camuffo, A. (2000). Del Vecchio e Luxottica. Torino: Isedi.

Buterin, V. (2014). "A next-generation smart contract and decentralized application platform." white paper.

Byrne, PM (2007). "Mastering Supply Chain Security". Logistics Management 46:25.

CargoX team (2018). "Business Overview and Technology Bluepaper"

Charts.bitcoin.com. (2018). Bitcoin.com. [online] Available at: https://charts.bitcoin.com/chart/blockchain-size [Accessed 15 Sep. 2018].

Chaum, D. (1983). "Blind signatures for untraceable payments" Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203.

Cohen, R. (2005) “Acceptable Knockoffs”. Time Magazine May 24.

Comelli M. (2008). “A combined financial and physical flows evaluation for logistic process and tactical production planning: Application in a company supply chain” Int. J. Production Economics 112 (2008) 77–95.

Credits’s blog [online] Available at: https://medium.com/@credits/how-blockchain-could-help-logistics-c3b2ab60be55 [Accessed 24 Jun. 2018].

Demirors, M. (2017). Leaders Series: Jessi Baker @ Provenance – The Future Collective – Medium. [online] Medium. Available at: https://medium.com/the-future-collective/women-in-blockch
ain-jessi-baker-provenance-67c70330d9a7 [Accessed 13 Jun. 2018].

DHL Trend Research (2018). “Blockchain in Logistics. Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry”.

Digiconomist. (2018). Bitcoin Energy Consumption Index - Digiconomist. [online] Available at: https://digiconomist.net/bitcoin-energy-consumption [Accessed 30 Aug. 2018].

En.bitcoin.it. (2018). Block size limit controversy - Bitcoin Wiki. [online] Available at: https://en.bitcoin.it/wiki/Block_size_limit_controversy [Accessed 17 Jun. 2018].

En.wikipedia.org. (2018). Hyperledger. [online] Available at: https://en.wikipedia.org/wiki/Hyperledger [Accessed 3 Jul. 2018].

Ganz, B. (2017). [online] Available at: http://www.ilsole24ore.com/art/impresa-e-territori/2017-05-02/luxottica-mette-disposizione-bonus-vita-e-banca-ore-etica- 093248.shtml?uuid=AEQgogEB [Accessed 15 Aug. 2017].

Geiger-Oneto Stephanie (2007). Elite Brands and Their Counterfeits: A Study of Social Motives for Purchasing Status Goods. Dissertation, University of Houston.

Greenspan, G. (2015). “MultiChain Private Blockchain - White Paper”.

Groenfeldt, T. (2017). “IBM And Maersk Apply Blockchain To Container Shipping”.

IBM FinTech: Asia. (2018). IBM FinTech: Asia. [online] Available at: https://www.ibm.com/think/fintech/maersk-and-ibm-form-joint-venture-applying-blockchain-to-improve-global-trade-and-digitize-supply-chains/ [Accessed 10 Sep. 2018].

Lucchetta, 2016. Logistics service optimization - The case of Luxottica. Milano: Polimi.

Luxottica (2007). Oakley To Merge Into Luxottica Group For Us$29.30 Per Share. [online] Luxottica. Available at: http://www.luxottica.com/en/oakley-merge-luxottica-group-us2930-share [Accessed 28 Jul. 2018].

Luxottica (2017). Dati divisione. [online] Available at: http://www.luxottica.com/it/investitori/highlights-finanziari/dati- divisione [Accessed 14 Aug. 2017].

Maupin, J. (2017). Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies. Centre for International Governance Innovation, pp.1-4.

Medium. (2016). Fluent Rebrands as Hijro! – Hijro – Medium. [online] Available at: https://medium.com/@Hijro/fluent-rebrands-as-hijro-71b98483d2bd [Accessed 16 Aug. 2018].

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System".

Needham & Company, LLC (2015) “The Blockchain Report: Welcome to the Internet of Value”

Okazaki, Y. (2018). Unveiling the Potential of Blockchain for Customs. [ebook] Available at: http://www.wcoomd.org/-/media/wco/public/global/Pdf/topics /research/research-paper-series/45_yotaro_okazaki_unveiling_the_Potential _of_blockchain_for_customs.pdf?la=fi [Accessed 7 Jul. 2018].

Pruksasri, P., van den Berg, J., Hofman, W., & Tan, Y. H. (2014). “Data concealing of supply chain transactions using the Distributed Trust Backbone.” In Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for (pp. 151-156). IEEE.

Pruksasri, P., van den Berg, J., Hofman, W., & Tan, Y. H. (2016). Enhancing process visibility of the supply chain 'data pipeline'. ECTI Transactions on Computer and Information Technology (ECTI-CIT), 10(1), 15-25.

Repubblica (1999). la Repubblica/fatti: Ray Ban, il marchio diventa italiano. [online] Repubblica.it. Available at: http://www.repubblica.it/online/fatti/rayban/rayban/rayban.html [Accessed 14 Jun. 2018].

Research.ibm.com. (2018). Crypto-anchors and Blockchain - IBM Research - US. [online] Available at: https://www.research.ibm.com/5-in-5/crypto-anchors-and-blockchain/ [Accessed 7 Feb. 2018].

Rowley, J. (2018). 2018 VC investment into crypto startups set to surpass 2017 tally. [online] TechCrunch. Available at: https://techcrunch.com/2018/03/03/2018-vc-investment-into-crypto-startups-set-to-surpass-2017-tally/?guccounter=1 [Accessed 12 Sep. 2018].

Sacchi, M. (2016). Luxottica, le redini a Del Vecchio: «Dobbiamo essere più veloci» [online] Available at: http://www.corriere.it/economia/16_gennaio_29/luxottica-redini-del-vecchio-dobbiamo-essere-piu-veloci-354419e0-c6cf-11e5-bc00-4986562dd09c.shtml. [Accessed 13 Aug. 2017].

Seppälä, J. (2016). "The role of trust in understanding the effects of blockchain on business models"

Skinner, C. (2016). "ValueWeb: How fintech firms are using mobile and blockchain technologies to create the Internet of Value".

Stella, G. (1996). Schei. Milano: Baldini & Castoldi.

Szabo, N. (December 2005). "Bit gold"

Takahashi, K., (2016), "blockchain technology and electronic bill of lading" available at https://www1.doshisha.ac.jp/~tradelaw/PublishedWorks /BlockchainTechnologyElectronicBL.pdf.

White, M. (2018). Digitizing Global Trade with Maersk and IBM - Blockchain Unleashed: IBM Blockchain Blog. [online]. Available at: https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/ [Accessed 18 Aug. 2018].

Williams-Grut, O. (2018). Only 48% of ICOs were successful last year — but startups still managed to raise $5.6 billion. [online] Business Insider. Available at: http://uk.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1?IR=T [Accessed 12 Jun. 2018].

Zeliha, E. (2014). “Counterfeit Supply Chains”. 2ND Global Conference of Business Economics, Management, and Tourism, Prague, Czech Republic.

Zhang, Y. (2011). “Approaches to Resolving the International Documentary Letters of Credit Fraud Issue”. University of Eastern Finland.