

Freie wissenschaftliche Arbeit
Zur Erlangung des Masters Engineering Management
an der Technischen Universität Berlin

Logistics oriented analysis of the integration of Blockchain and Internet of Things

Eingereicht beim

Bereich Logistik

Tino Herden, M.Sc.

Von

Cand.-M.Sc Eduard Delmás

Matr.-Nr: 240272

Coppistr.16

10365 Berlin

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne unerlaubte fremde Hilfe angefertigt, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzen Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Berlin, 17.09.2018

Abstract

This thesis's purpose is to make an in-depth analysis about Blockchain (BC) and Internet of Things (IoT) technologies. Characteristics, purpose and use cases from these two fields will be studied individually and afterwards a research about how can they interact both in a general and also a logistic-oriented point of view will be conducted. The issue will be addressed by summarizing the latest scientific literature, consisting on a systematic review of articles and papers from prestigious institutions and authors announcing the current state of the art of IoT and Blockchain.

Content

Abstract.....	3
Figure summary	6
1. Introduction	8
1.1 Objectives and expected results.....	10
2. Theoretical background.....	11
2.1 Blockchain.....	11
2.1.1 Mechanics of the Blockchain	11
2.1.2 Theoretical Potential	19
2.1.3 Sectorial applications	20
2.1.4 Blockchain's utility.....	24
2.1.5 Possible logistic applications	25
2.1.6 Real use cases	28
2.2 Internet of Things	30
2.2.1 Mechanisms of the IoT	31
2.2.2 Theoretical potential.....	37
2.2.3 Possible logistic applications and related use cases	47
2.3 Interaction models.....	51
2.3.1 Possible frameworks	52
2.3.2 Framework evaluation and selection	53
2.3.3 Specific model development	54
3. Methodology	56
3.1 Inclusion criteria	57
3.1.1 Flaws and limitations over the inclusion criteria.....	57
3.2 Model application	57
3.2.1 IoT elemental challenges	58
3.2.2 Blockchain basic use cases	60
3.2.3 IoT Challenge Blockchain use cases match	61

3.2.4	Advantages versus centralized databases	67
3.2.5	Use scope: Logistics	70
4.	Results	73
5.	Discussion	76
5.1	Criticism	76
5.2	Future research	78
6.	Final remarks	80
	Bibliography	82

Figure summary

Figure 1: Total Cryptocurrency market evolution and daily volume. From 31th Dec 2015 to 30th Jul 2018.....	11
Figure 2: Hash conversion given two different data inputs through Message-Digest Algorithm 5.....	12
Figure 3: Block example: (1) Index, (2) Timestamp, (3) Previous and Current Hash, (4) Data input, (5) Nonce.	13
Figure 4: Three blocks Blockchain where every block hash starts with three 0's and therefore it's valid (green).....	14
Figure 5: Invalidation of one block and its successive ones by changing the input data.	15
Figure 6: Same Blockchain shown in Figure 5. This time the blocks are valid since they were mined and a new Nonce was found.	16
Figure 7: Same Blockchain record for three peers. The third one (right) is not valid because it does not match the values from the majority of users.....	17
Figure 8: Possible combination of Blockchain implementations based on the access given to read and add data into the Blockchain. (Source: Bitfury).....	19
Figure 9: Summarizing possible sectorial Applications for Blockchain.	22
Figure 10: Main differences between a Permissionless Blockchain, a Permissioned Blockchain and a Central Database. (Source: ETH Zurich)	24
Figure 11: Decision tree in order to decide if Blockchain as a data base type makes sense in a given situation or not. (Source: ETH Zurich).....	25
Figure 12: Comparison between a Traditional and a Blockchain powered SCM scheme. (Source: ETH Zurich)	26
Figure 13: Communication as the key to allow the specific properties from an IoT network of given devices to work.....	33
Figure 14: Communication Device-to-device.	33

Figure 15: Connection between devices through a Network with an entrance and exit gateway.....	34
Figure 16: Connection between devices through a Network with no gateway requirements.	34
Figure 17: IoT's architecture graphical representation.	36
Figure 18: Main IoT Applications divided by sector.....	44
Figure 19: Summarizing the core technologies for IoT which could push it forward and its required scientific developments. (Source: K. Patel, S. Patel).....	45
Figure 20: IoT major challenges and adoption barriers dissected into elemental issues.	60
Figure 21: Blockchain basic use case dissection.....	61
Figure 22: Matching IoT correct challenges with Blockchain use cases.....	62
Figure 23: Found matches between IoT challenges and Blockchain use cases.....	68
Figure 24: Kodak's stock price in USD. Sep'2017-Sep'2018. (Source: Yahoo Finance)	77

1. Introduction

The term Internet of Things was originally coined in 1999 by Kevin Ashton as a way to link internet as a useful tool with P&G's supply chain. He did not define an accurate description for the term, but he spoke about the big dependence which computers had on humans and the inefficiency that this fact entails. If computers were able to gather data without any help from humans, we would be able to greatly decrease waste, loss and cost in many logistic processes¹. Today, IoT is a trending topic on the scientific and industrial world and have many definitions. In a report by McKinsey it is described as sensors and actuators connected by networks to computing systems. These systems can monitor or manage the health and actions of connected objects and machines. Connected sensors can also monitor the natural world, people, and animals². Almost 20 years later from that conference, we are still using a fraction from all the data that we gather and it is mainly used as a control tool (alarms, real-time indicators...) rather than for optimization and prediction³.

Growth perspectives around the IoT are very promising, but there is as well a wide variety of opinions within this good scenario. As of today, an amount of somewhere between 6,4 billion and 9 billion IoT devices (without including smartphones, tablets and computers) and 17,6 billion (including them) are estimated. Many experts on the field claim that by 2020 there will be around 20-30 billion devices.⁴ Despite de these great growth projections, companies do still have many concerns about the subject. Main ones are ensuring privacy, regulatory compliance, acquiring the needed skills to leverage IoT data, managing the growing volumes of data and securing IoT sensors and their data.⁵

Those concerns in regard of Internet of Things brought the idea to study a possible interaction of this technology with Blockchain in an attempt to find a symbiotic solution. Blockchain was firstly applied in 2009 in the original Bitcoin white paper created by Satoshi Nakamoto, who defines this technology as a chain of digital signatures.⁶ Essentially, Blockchain is a database type for recording transactions where every

¹ Kevin Ashton, 2009, p. 1.

² James Manyika and others, 2015, p. 9.

³ Manyika and others, 2015, p. 9.

⁴ Amy Nordrum, 2016; Chin-Lung Hsu and Judy Chuan-Chuan Lin, 2016, p. 1.

⁵ Harvard Business Review, 2014, fols 3–4.

⁶ Satoshi Nakamoto, 2008, p. 1.

transaction is copied to all of the computers in a participating network.⁷ Every elemental structure from this chain where data is stored is called a block⁸ and every block contains information in regard of previous -in a chronological sense- blocks. Thus in order to modify the information contained in one of those blocks it is required to change every previous one.⁹ This Blockchain property permits the user to rely on a decentralized environment which provides irrefutable historic data and information.

This technology firstly created in order to allow online payments to be sent directly from one party to another without going through a financial institution offers nowadays many other possibilities. As of today, even by being two cutting edge technologies, it is possible to find some companies and business models which try to use Blockchain properties in order to make the most out of IoT and eliminate those concerns described above. Examples of that could be VeChain, WaltonChain or WaBi. As it can be observed, many companies that combine these two technologies use Blockchain to improve IoT attributes and mainly fight the lack of trust, security and confidence that the later provides. Moreover, cited companies use the Blockchain and IoT mix in order to fulfil a supply chain task. In VeChain case, as an example, these combined technologies are employed in order to control and validate the authenticity of a product during its distributing process. By understanding the underlying value and characteristics it is easy to figure out why those companies choose to solve these security and trust challenges through the Blockchain. Some of this theoretically possible benefits are listed below¹⁰:

- Blockchain can be used to prevent duplication with any another malicious data
- Blockchain is well suited to simplify complex IoT device deployments by identifying, authenticating and securing data transfer
- There's no more need to use a third party to assure trust
- It is possible to eliminate the single source of failure chance
- Thanks to Smart Contracts it is possible to increase device autonomy, integrity of data and supports peer to peer communication.
- In some cases, using Blockchain can improve efficiency and reduce costs

⁷ Bob Alice, 2016, p. 5.

⁸ Nakamoto, 2009, fols 2–4; Alice, 2016, p. 5.

⁹ Nakamoto, 2009, fols 2–4.

¹⁰ Khwaja Shaik, 2018.

However, Blockchain implementation has some drawbacks as well since for it to work properly it is required a large and widely distributed network, it may lead to high transaction costs and low speed within them.

In this thesis it is expected to carry out a deep analysis of both technologies, on an individual and a combined level, considering its possible benefits and drawbacks both for a general and a logistic-oriented scenario.

1.1 Objectives and expected results

As objectives for this thesis, it is expected to:

- Analyse the characteristics and applications of both technologies on an individual level.
- Follow a standardized methodology in order to systematically review the possible interactions between IoT and Blockchain.
- Analyse the possible real use case scenarios where the found interactions could be applied both on a general and a logistic oriented perspective.

Regarding the results, it is expected that this thesis will help to better understand the IoT and Blockchain purposes, benefits and use cases both on an individual and combined level. Furthermore, and following a rigorous approach, it's expected as well to map the real value beyond the expectations and to detect the obstacles and challenges which this technological interaction is facing nowadays.

2. Theoretical background

2.1 Blockchain

In 2009, Satoshi Nakamoto published his famous paper “Bitcoin: A peer-to-peer electronic cash system”, where he explains his vision about creating an environment which allows online payments to be sent directly from one party to another without going through a financial institution¹¹. A few years later, it became evident that the underlying technology that operated bitcoin could be separated from the currency itself and that it could be used for all kinds of other purposes. Nowadays we understand this technology as Blockchain.

During the last years, and mostly during 2017, Blockchain technology as well as cryptocurrencies –such as Bitcoin or Ethereum- and other related companies became really famous, and it experienced a large growth, with a peak of over 800B\$¹² (Figure 1) at the end of the past year for the whole cryptocurrency market. As a reference to better understand this number, even if it's not fair to compare a company's market capitalization with the one from a currency, Apple, the biggest company in the world by capitalisation, is slightly over 900B\$¹³. Due to this extremely fast growth, it captured the attention from media, investors, companies and Start-ups from all over the world, creating a kind of new and contemporary gold rush. Despite this, this thesis will aim to map the value beyond the hype, starting from the technological point of view.



Figure 1: Total Cryptocurrency market evolution and daily volume. From 31th Dec 2015 to 30th Jul 2018.¹⁴

2.1.1 Mechanics of the Blockchain

As announced in the previous introduction, Blockchain is, as its own name indicates, a database type conformed by a chain of blocks where every block contains information in regard of previous ones -implying that in order to modify the information contained in one of those blocks it is required to change every previous one- and they are used to record

¹¹ Nakamoto, 2009, p. 1.

¹² 'CoinMarketCap', 2018.

¹³ 'Apple Inc. (AAPL)', 2018.

¹⁴ 'CoinMarketCap', 2018.

transactions where every transaction is copied to all of the computers in a participating network.¹⁵ This Blockchain property permits the user to rely on a decentralized environment which provides irrefutable historic data and information.


However, that general definition relies on different concepts which need to be further explained in order to truly understand the technology. Those basic elements are Hash, Block, Blockchain and Decentralization.

2.1.1.1 The Hash

A hash is a very efficient mathematical function which converts strings of almost arbitrary length to strings of a short fixed length. Given different uses and applications the hash might present different properties, but there are a few that are necessary for the hash to be¹⁶:

- The conversion is always supposed to be one way, meaning that it's almost impossible in practice to find the original data string given a hash.
- The hash provides the data with a unique fingerprint, meaning that it uniquely identifies it. Therefore, in a practical way two different data inputs will outcome in two different hash values.

To better illustrate that, in the Figure 2 it is possible to observe an example created with a cryptographic tool which allows to convert data into a hash through MD5 (Message-Digest Algorithm 5) which is a cryptographic algorithm widely used¹⁷. It's possible to notice too that with a little change in the input data, we obtain a completely different hash, thus small changes in data generate big changes in the subsequent hash.



Your Hash: 81856c4b5e677e500558ad74dc09521c Your String: TU Berlin
Your Hash: 4baeb6c3b07f2aa67c3fde6f894a43b3 Your String: TU Berlin 2018

Figure 2: Hash conversion given two different data inputs through Message-Digest Algorithm 5

Hash functions have many applications –and therefore many properties- in a wide variety of fields. Nevertheless, being the aim of this chapter the Blockchain's cryptographic

¹⁵ Nakamoto, 2009, fols 2–4.

¹⁶ Søren Steffen and Lars Ramkilde, 2009, fols 2–3.

¹⁷ 'Md5hashgenerator', 2018.

background explanation, it's possible to state three basic requirements, which a Hash function needs to meet¹⁸:

- **Collision resistance:** Implies the almost practical impossibility to find two data inputs which result on the same hash value.
- **Preimage resistance:** Implies the almost practical impossibility of finding a valid data input given a specific hash value.
- **Second preimage resistance:** Given a data input, it implies the almost practical impossibility of finding another data input that results on the same hash.

2.1.1.2 The Block

Understanding now that a Hash is a function of a given string of data, a Block is a function of many factors (Figure 3):

- **Index:** The Index is the position of the block in the chain (The genesis block has an index 0, the next one 1, the next one 2 and so on).
- **Timestamp:** The Timestamp is a record of when the block was created and help to keep the Blockchain in order.
- **Actual and Previous Hash:** It contains the hash from the previous block as well as the one derived from the actual one.
- **Data:** The actual data that we put on the block (for example, in the case of Bitcoin those are currency transactions)
- **Nonce:** Is the number that makes the current block valid. That translates into a hash that meets a certain requirement. In the example that we will see later on, a valid hash will consist in one starting by three 0's, and in order to find this number the Nonce iterates from 0 until a valid hash is found by using processing power.



Figure 3: Block example: (1) Index, (2) Timestamp, (3) Previous and Current Hash, (4) Data input, (5) Nonce.

¹⁸ Steffen and Ramkilde, 2009, p. 3.

2.1.1.3 The Blockchain

The Blockchain, as a self-explanatory concept, consists on a list of successive blocks. Every block receives a hash in regard of the data it contains, and within this data we find the hash from the previous block as one of its elements. Therefore, if any kind of change or alteration is produced in a previous block, the hash from every successive block will be altered too. Those hashes will lose their three initial 0's -which is the requirement established in this thesis for a block to be valid, but it can be a completely different one- and therefore the block will be considered as invalid. Nevertheless, it is still possible to validate those blocks again by finding a new Nonce that makes the hash start by three 0's. That process is defined as mining. As a way to illustrate that, in the Figure 4 it is possible to observe a sequence of three blocks, where everything is alright and the data introduced in each one is "TU Berlin", "TU Berlin 1" and "TU Berlin 2".

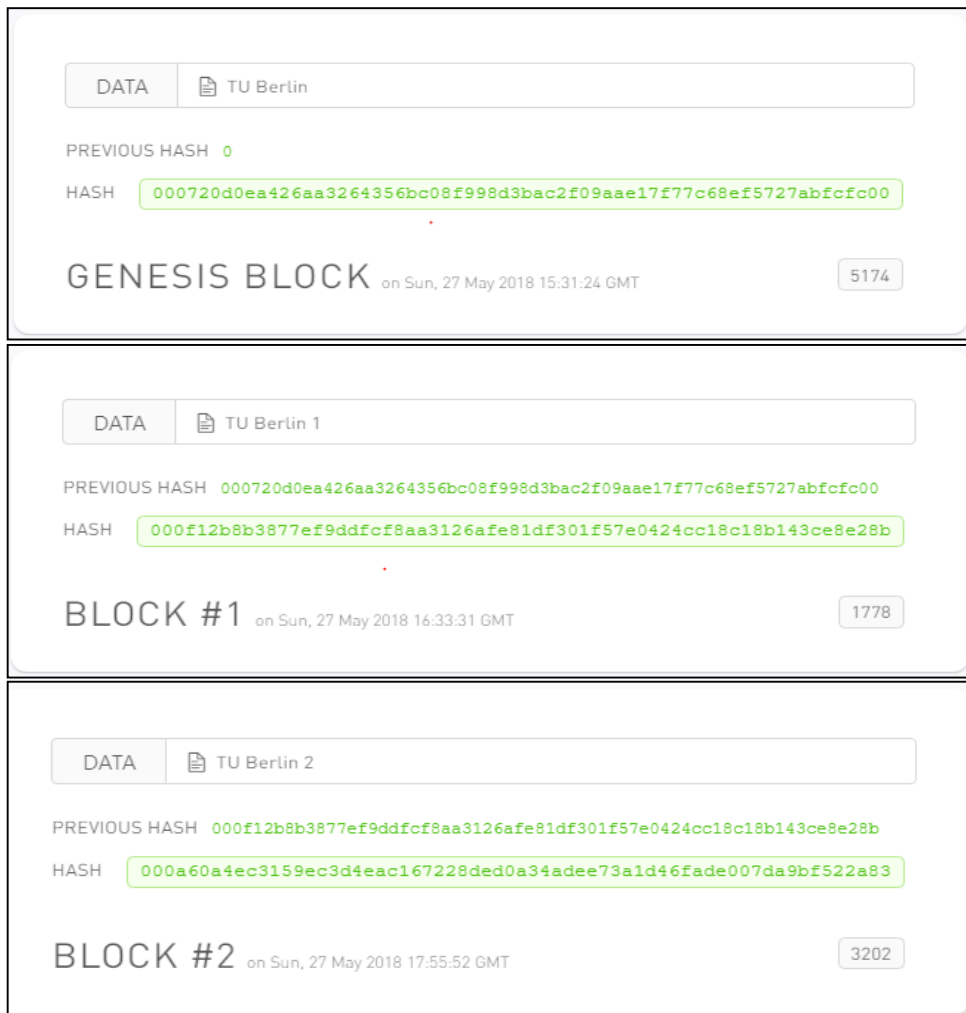


Figure 4: Three blocks Blockchain where every block hash starts with three 0's and therefore it's valid (green).

Following with this example, if the data from the first block -Block #1 and not the Genesis Block- is altered by replacing “TU Berlin 1” with “Faculty VII” (Figure 5), the hash from this very block turns out to be invalid as it does not start with the three 000’s. Therefore, following the logic of the Blockchain’s properties explained above, the next block –the second- is invalidated as well.

The image displays three blocks from a blockchain interface, stacked vertically. Each block has a 'DATA' field with a document icon and a text input field. Below the data field are 'PREVIOUS HASH' and 'HASH' fields. The 'HASH' field in each block is highlighted with a colored border: green for the Genesis Block, red for Block #1, and red for Block #2. The Genesis Block is labeled 'GENESIS BLOCK' and has a timestamp of 'on Sun, 27 May 2018 15:31:24 GMT' and a value of '5174'. Block #1 is labeled 'BLOCK #1' and has a timestamp of 'on Sun, 27 May 2018 16:33:31 GMT'. Block #2 is labeled 'BLOCK #2' and has a timestamp of 'on Sun, 27 May 2018 17:55:52 GMT'. Each block also features a blue circular share icon in the bottom right corner.

Block	Data	Previous Hash	Hash	Timestamp
Genesis Block	TU Berlin	0	000720d0ea426aa3264356bc08f998d3bac2f09aae17f77c68ef5727abfcfc00	on Sun, 27 May 2018 15:31:24 GMT
Block #1	Faculty VII	000720d0ea426aa3264356bc08f998d3bac2f09aae17f77c68ef5727abfcfc00	dfe4e3843cd72a601427b799c6c2a686ae744cbc057ea9c13350314d2a6036a9	on Sun, 27 May 2018 16:33:31 GMT
Block #2	TU Berlin 2	dfe4e3843cd72a601427b799c6c2a686ae744cbc057ea9c13350314d2a6036a9	bcf1ebf9a7c2a95dd4a3e5dc09cd03fd3047d1edc0f9ad18d3dc3bc5a14f4510	on Sun, 27 May 2018 17:55:52 GMT

Figure 5: Invalidation of one block and its successive ones by changing the input data.

In order to validate those blocks again (Figure 6), as said previously, it's necessary to mine them to find a proper Nonce. As the only requirement in this example is to match three 0's in the block's hash beginning, it's quite easy to do so –implying that it requires low computing capacity-, but it's possible to make it as complicated as desired.

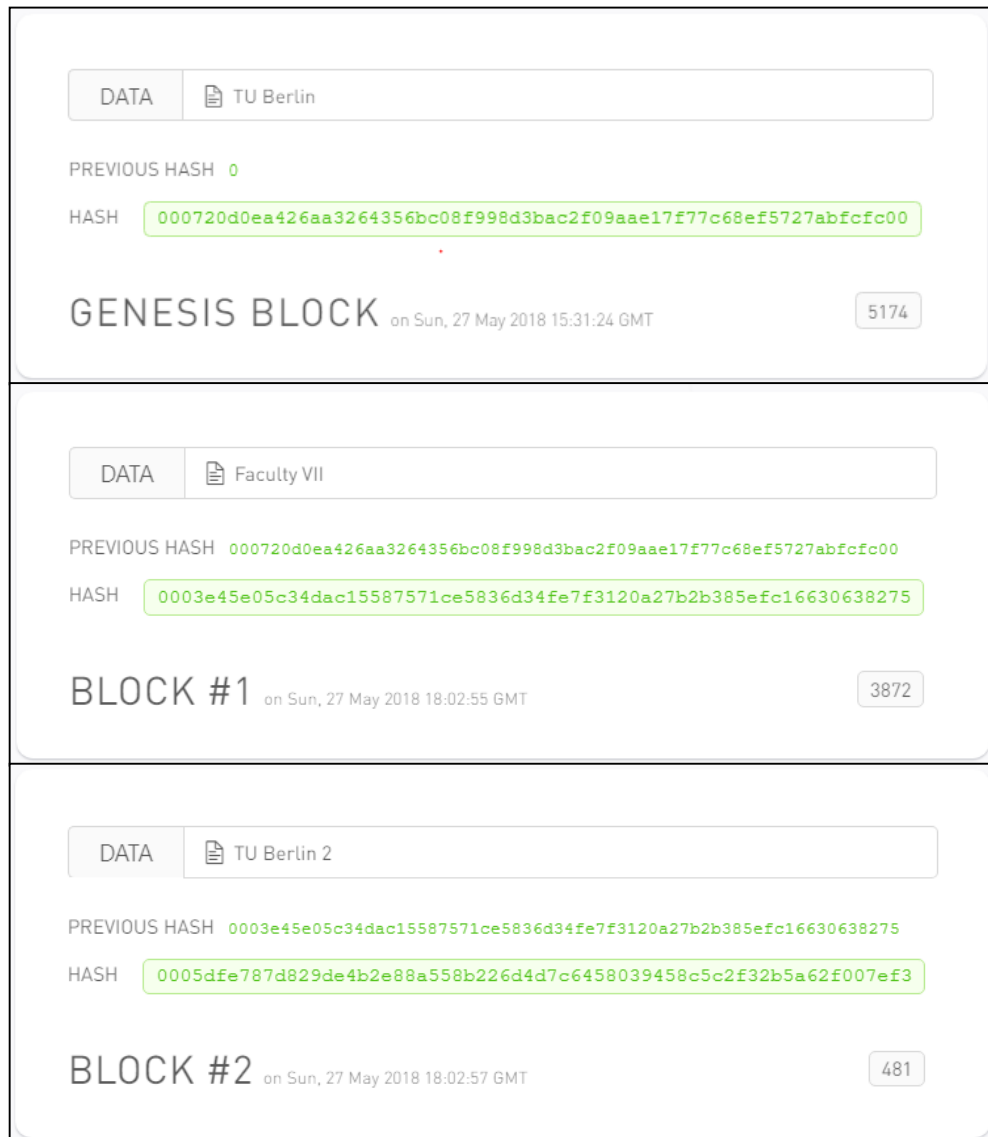


Figure 6: Same Blockchain shown in Figure 5. This time the blocks are valid since they were mined and a new Nonce was found.

This simple yet good explanatory example proves that it's actually possible to change the information within a Blockchain, apparently losing its invariability property. But that's where the famous decentralization comes to play along.

2.1.1.4 The Decentralization

Decentralization makes reference to a peer-to-peer Network, where a global network of computers works together to keep the Blockchain secure, correct and consistent. Instead of relying on an intermediary among them, they agree on a protocol called a consensus algorithm, which enables them to establish mutual trust and allows for validating –against the validation rules that are set by the creators- the transactions on a peer-to-peer

basis.¹⁹ Besides that, given a Blockchain if some party tries to alter the data from a determined block, that block will be detected as invalid as the majority of the users will have other values. In order for someone to make a change in the Blockchain, it needs to have more than the 51%²⁰ of the computing capacity, and if the network is distributed worldwide, that's unlikely to happen.

In order to clarify that point, the following example was created. Given a Blockchain with three peers, one of those three users alters the data from one block -from "TU Berlin 1" to "Faculty VII"- which is automatically detected as invalid, as the majority –in this case, two thirds- of them agree on other values. (Figure 7).

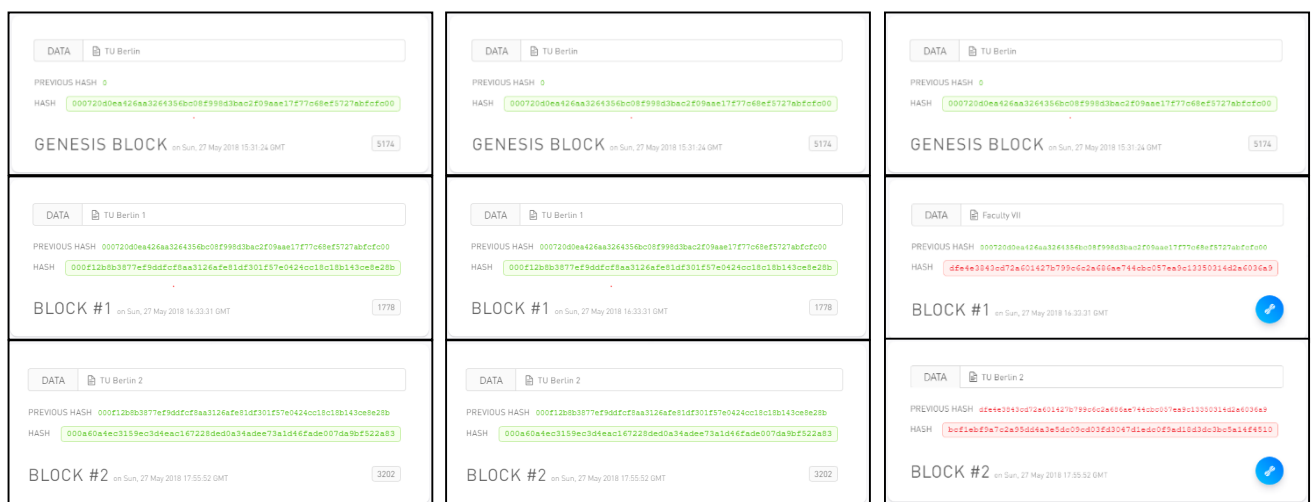


Figure 7: Same Blockchain record for three peers. The third one (right) is not valid because it does not match the values from the majority of users.

It is important to say, that this example was created using a Proof of Work system as a consensus method where every user owns the same proportional computing capacity. This consensus method together with the other existing ones are briefly explained in the next chapter.

2.1.1.4.1 Consensus Methods

Being the Blockchain an open ledger where everyone is allowed to introduce new information, the possibility of a fraudulent actor trying to add false information (such as double spending) is undoubtedly high. Therefore, consensus methods are used to allow all the parties from a given network to come to an arrangement on what true information

¹⁹ Deepak Puthal and others, 2018, fols 1–3.

²⁰ Puthal and others, 2018, p. 2.

is.²¹ Since the urge of Bitcoin many consensus methods with different background ideas have been developed. Nevertheless, the two most utilized and well-known ones are explained below:

- **Proof of Work (PoW)**²²: Every participant wishing to add a block into the Blockchain needs to solve a computational problem which requires a determined amount of computational capacity and therefore, electricity and money. All the participants compete to be the first in solving the puzzle since the network offers a reward for the one who succeeds. Therefore, all the participants are continuously verifying and validating the solutions that are proposed. According to that, to create a fraudulent transaction, which would be immediately invalidated by other users, would still carry an economic cost. Hence as long as the majority (51%) of the computing power remains controlled by honest parties, the system will be valid over the long term.
- **Proof of Stake (PoS)**: If the capability of validating and adding a new block into the Blockchain in a PoW system depended on the computational capacity of the user, in PoS it depends on the amount of assets that this user possesses in regard of the totality. In order to do that, the participants need to put their currency at “stake”, meaning that if they do any kind of fraudulent transaction, that will be detected by the rest of participants and they will lose their capital. In that case, the participants do not receive a block reward but they collect the network fees.

Both methods have their own advantages and disadvantages. On the one hand, PoW allows everyone to be a miner even if they do not own any currency, discourages DDOS attacks since they imply an economic cost and every participant needs to contain a ledger of previous Blockchain transactions, embracing decentralization. Nevertheless, to solve those puzzles is extremely energy consuming –mainly because of the processors and cooling systems- and it does not seem sustainable in the long run because of its environmental impact (in 2013, the energy consumed towards bitcoin mining equalled that of the used in the country of Ireland)²³. On the other hand, PoS does not require any kind of computing capacity and therefore energy consumption, but it isn't as robust as PoW in defending the network against malicious attacks. Furthermore, PoS gives a higher reward to those users with the highest amount of currency at stake, creating an unbalanced environment for decentralization.

²¹ Julian Debus, 2017, p. 1.

²² Debus, 2017, fols 13–15.

²³ Debus, 2017, fols 17–18.

2.1.1.5 Implementation types

Before ending the technological section, it is required to explain the different implementation types in which a Blockchain can be classified. It can either be **public** or **private**, the first one implying that there are no restrictions on reading the contained data or submitting new transactions to be included into the Blockchain and the second one that just predefined entities have those rights. It can also be either **permissionless** or **permissioned**, the first one implying that there are no restrictions for any user to be eligible to add new blocks and the second one that this capability is held just by predefined users with known identities²⁴. Those concepts can be mixed creating four different scenarios (Figure 8²⁵).

By access to transactions	By access to transaction processing	
	Permissioned	Permissionless
Public	Proprietary coloured coins protocols	Existing cryptocurrencies (e.g, Bitcoin)
Private	Direct read/transaction creation access for clients and regulators. Access limited to transaction processors.	Not applicable

Figure 8: Possible combination of Blockchain implementations based on the access given to read and add data into the Blockchain. (Source: Bitfury²⁶)

2.1.2 Theoretical Potential

Understanding the basic underlying mechanisms behind Blockchain as a technology, this chapter will entail its theoretical potential in a general –not logistics wise- way. This new technology promises to disrupt business models and transform industries. Blockchain, is pulling us into a new era of openness, decentralization and global inclusion. It leverages the resources of a global peer-to-peer network to ensure the integrity of the value exchanged among billions of devices without going through a trusted third party. Unlike the internet alone, Blockchain is distributed, not centralized; open, not hidden; inclusive, not exclusive; immutable, not alterable; and therefore, secure. Theoretically, Blockchain gives us the capabilities to create and trade value in society, since it enables

²⁴ BitFury Group and Jeff Garzik, 2015, p. 10.

²⁵ BitFury Group and Garzik, 2015, p. 11.

²⁶ BitFury Group and Garzik, 2015, p. 11.

such innovations as artificial intelligence (AI), machine learning, the internet of things (IoT), robotics and even technology in our bodies, so that more people can participate in the economy, create wealth and improve the overall state of the industry.²⁷

Thanks to the described characteristics, Blockchain is able to offer us three main utilisations²⁸:

- **Storage of digital records:** Blockchain can be used to store digital identities of individuals, organisations, assets, titles and even voting rights. Essentially everything which can be represented digitally.
- **Exchange of digital assets:** Blockchain can execute peer-to-peer transactions without a trusted third-party intermediary, reducing times and related costs.
- **Recordation and execution of Smart Contracts:** Smart Contracts are digital codes that enable the automated execution of specified actions based on contractual conditions as validated by all parties. The easiest example is to think about the transaction system in Bitcoin, where the smart contract automatically checks before the transaction if the one sending money does have enough funds to do that, and If he does not, the transaction is invalidated. Basically it would be possible to auto-execute recurring business transactions and help to reduce contractual defaults.

By knowing the main applications which this technology entails, it's possible to study its possible sectorial usage based on the desired properties to exploit and the given problems to solve.

2.1.3 Sectorial applications

When someone thinks about possible applications and use cases for Blockchain as a technology, it's common to think only about the financial services industry, since it has been the pioneer sector and almost every big financial institution is working in collaboration with a Blockchain start-up or developing its own one.²⁹ Nevertheless, the possible appliance of Blockchain goes way beyond that. Below, different examples of how could this technology could be applied in different sectors are presented:

²⁷ Don Tapscott and Alex Tapscott, 2017, p. 4.

²⁸ Saurabh Mahajan, 2018, p. 2.

²⁹ IBM, 'Banking Use Cases', 2018; IBM, 'Financial Markets Use Cases', 2018.

- **Financial Services:** It allows international payments in a faster, cheaper and more secure way. An real use case example for that can be found in Ripple, which is already working with banks such as Santander³⁰ or SBI Group³¹. The technology could also be used as a KYC (know your customer) mechanism, in order to be completely aware of the checks and compliance given different situations.
- **Health care:**³² In this sector it's possible to define two main application branches. The first one is related with using smart contracts in order to connect different parties. That means that providers, insurers, vendors and auditors should be able to eliminate possible trust issues while automating different transactions. The other branch relies on the information exchanges. With Blockchain the disintermediation of trust would be possible, since no intermediary will be required –all the participants would have access to the distributed ledger to maintain a secure information exchange-. That's supposed to be able to reduce the transaction costs while allowing near-real time processing. Hence, making the whole information exchange more efficient.
- **Public sector:** In the public sector, by using Blockchain the authorities would have the capability of managing people's digital identity and attach ownership and transaction information on different assets such as real property and vehicles to increase efficiency and reduce fraud. Another interesting application would be to use Blockchain to carry out the public election voting process, enhancing the transparency and security of the event.
- **Energy and resources:**³³ The first application for this field consists on supporting the peer-to-peer trading for a smoother operation of the power grid. Aggregating Blockchain to Virtual Power Plants could reduce transaction costs through standardization via Smart Contracts and automating execution orders. The second possible application would be to optimise the supply chain and logistics of the sector. Nowadays all parties require continual consensus with other parties which usually use completely different information tracking systems leading to significant challenges for the optimization of the shipment process. An example for that would be to create a smart contract which confirms a payment from a selling party once a set of conditions is met. On the physical side, the electricity consumption is tracked with sensors and the values are linked to the

³⁰ Andy Smith and Cecilia Cran, 2015.

³¹ SBI Group, 2018.

³² RJ Krawiec and others, 2016, fols 1–3.

³³ Dutsch and Steinecke, 2017, fols 15–16 .

smart contract. Once this consumption is effectuated, the payment is automatically triggered through the execution of the contract.

- **Technology, media and telecom:** Those sectors are closely linked to Blockchain mainly because of the current ownership validation problem. Blockchain could allow the storage of cryptographic hashes belonging to original music, films, pictures, articles... and linking them to digital identities of owners, using smart contracts to facilitate the economic compensation for the content utilization. Another application would be to mitigate the security concerns within data storage. given a large network of IT devices.
- **Consumer and industrial products:** Blockchain could be extremely useful by streamlining and smothering processes such vehicle buying and leasing, allowing automated payments and reducing the amount of needed documentation. The technology could help as well to enhance the supply chain management, increasing the traceability across products from its inception at manufacturer to usage by end costumer. Lastly, it could improve the management of loyalty points programs in retail, travel and hospitality.

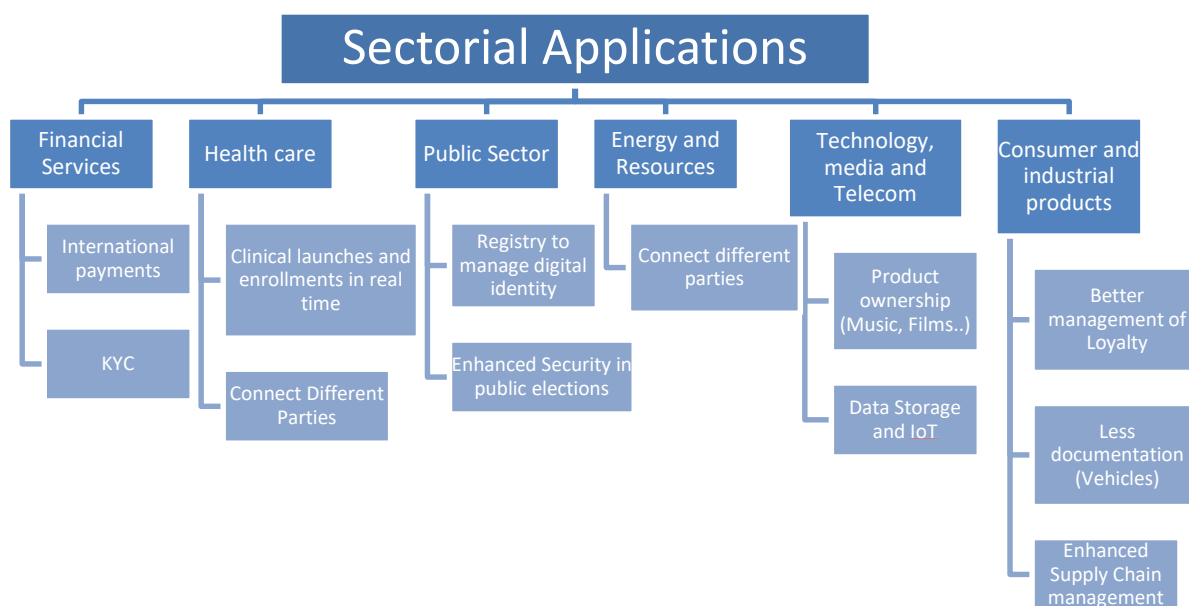


Figure 9: Summarizing possible sectorial Applications for Blockchain.

As it can be observed, many of the applications provided by Blockchain for the described sectors are strictly related with the logistics of the sector itself. That's because one of its main applications it's to put many parties to rely in a unique source of truth, among others. However, Blockchain as an almost brand new technology needs to overcome many challenges and to leverage in its key drivers in order to succeed and achieve general adoption.

2.1.3.1 *Key drivers and Challenges*

Firstly, taking a look at the key drivers which push Blockchain forward as a technology, it's possible to distinguish three core ones³⁴:

- **Lower costs of bandwidth, data storage and computing capacity:** This permits Blockchain to act in a fluid way and embrace new users.
- **More efficient way to maintain trust:** Something very important nowadays within almost every digital business model is to maintain a good trust level towards the user and Blockchain permits to do so in a more efficient way. For example, a large business consortium with many parties where every party keeps track of the transactions could use a unique Blockchain as a single source of truth.
- **Prevalence of decentralized business models:** With the recent expansion of the sharing economies, Blockchain seems like a good idea for those business models to really democratize the value exchange in those economies business models by removing the need for centralized aggregators –imagine an AirBnb without AirBnb in the middle-.

Secondly, speaking about drawbacks or challenges, it's possible to find four main reasons, partly related to the fact of the technology being very new and the market immature³⁵:

- **Low awareness and understanding:** According to a Deloitte's survey³⁶, 39% of senior executives in large US organizations have little-to-non knowledge in regard of Blockchain. This is a principal challenge because there is low understanding of how could this technology be applied to a particular business model in order to improve it or make it more efficient.
- **Lack of standards and best practices:** There is few standardizations among industry players in order to homogenize the Blockchain environment. There is a need to build uniform standards and protocols, rather than develop internal versions, in order to embrace a wider adoption.
- **Mass adoption is a requirement for mass adoption:** The adoption of foundational technologies typically happens in four phases: Single use,

³⁴ Mahajan, 2018, p. 4.

³⁵ Mahajan, 2018, p. 5; Marco Iansiti, Karim R Lakhani, and Hassan Mohamed, 2017, fols 7–9.

³⁶ Mahajan, 2018, p. 5.

Localization, Substitution and Transformation. This whole process can take up to decades to transform the economy. Blockchain, as said before, is very useful when putting different parties together without an intermediary in order to assure trust among them. Therefore, if some of those parties do not have the capabilities, opportunities or desire to join within this new technology, the creation of a Blockchain network will have little-to-non-use.

- **Regulatory and legal uncertainty:** An unusual situation is given whenever the law and regulations are able to keep pace with the advances in technology. With Blockchain is not different and the current uncertainty towards this technology's regulation in regard of applications such as smart contracts or digital identities are for sure not boosting its wider adoption.

2.1.4 Blockchain's utility

As usual with new technologies with ground-shaking promises, there is a lot of hype and overreaction –as well as scepticism- wrapping it like a fog cloud which does not allow the public and potential users to see clearly through it in order to understand its intrinsic properties and purposes. This chapter aims to clarify in which occasions and situations does Blockchain make sense in comparison with the conventional data bases that we have been using so far. As a final remark, it's required to be said that in order to understand this chapter, the concepts explained in the previous section 2.1.1.5 Implementation types are undoubtedly indispensable to be known.

	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	PoW, PoS	BFT protocols	None
Centrally managed	No	Yes	Yes

Figure 10: Main differences between a Permissionless Blockchain, a Permissioned Blockchain and a Central Database. (Source: ETH Zurich)

There are some clear premises such as if no data needs to be stored, no data base is required at all and therefore, Blockchain makes no sense. In the same way, if there is only one writer a Blockchain makes again no sense, since a centralized database will provide better performance in terms of throughput and latency.³⁷ Nevertheless, there are some scenarios which remain more unclear and require of further thought (see Figure 11³⁸ for a better understanding). Generally speaking, using an open or permissioned Blockchain is just useful in the case of multiple mutually mistrusting entities that want to interact and they do not agree on a trusted third party. When comparing the technical properties among Central Database and a Permissionless or Permissioned Blockchain (Figure 10³⁹), it's possible to observe that the first one possesses a much better performance in terms of latency and throughput, since it does not require a consensus mechanism. On the other hand, Blockchain could provide better scalability and the elimination of a trusted third party (TTP). As a final remark, when making a decision of whether to use Blockchain or not, all these elements should be taken under consideration.

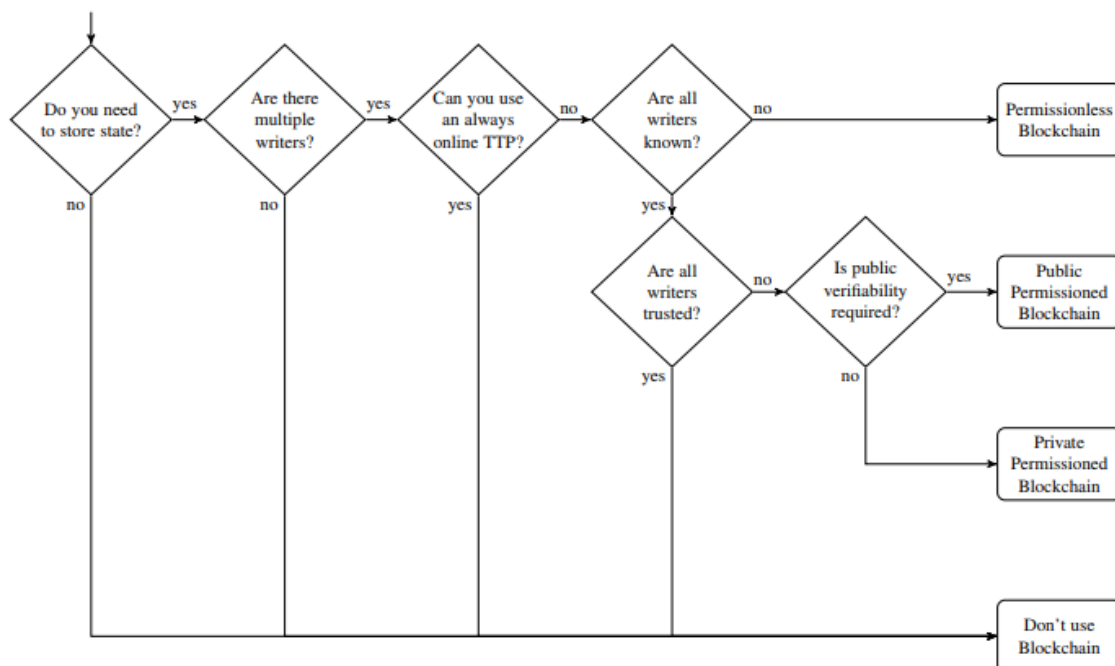


Figure 11: Decision tree in order to decide if Blockchain as a data base type makes sense in a given situation or not. (Source: ETH Zurich)

2.1.5 Possible logistic applications

As it can be observed, many of the applications provided by Blockchain described in the section 2.1.3 Sectorial applications are strictly related with the logistics of the sector itself.

³⁷ Karl Wüst and Arthur Gervais, 2017, p. 2.

³⁸ Wüst and Gervais, 2017, p. 3.

³⁹ Wüst and Gervais, 2017, p. 3.

That's because one of its main applications is to put many parties to rely in a unique source of truth, among others.

Managing today's supply chains —all the links to creating and distributing goods— is extraordinarily complex. Depending on the product, the supply chain can span over hundreds of stages, multiple geographical (international) locations, a multitude of invoices and payments, have several individuals and entities involved, and extend over months of time. Due to the complexity and lack of transparency of current supply chains, there is interest in how Blockchain might transform the supply chain and logistics industry.⁴⁰ Therefore, within this industry and taking into consideration the characteristics of the technology explained so far, it is possible to find the following main applications⁴¹:

- **Faster and Leaner Logistics in Global trade:** Global trade implies a really large number of parties involved, which often creates a conflict in interests and priorities (Figure 12). The conflicts in procurement, transportation management, track and trace, customs collaboration and trade finance could be easily alleviated. Maersk and IBM are already working on an end to end shipment tracking system Blockchain based. World economic forum says⁴², that if we are able to remove those barriers in the supply chain on a global level, the global GDP would be increased in a 5% just from doing that.

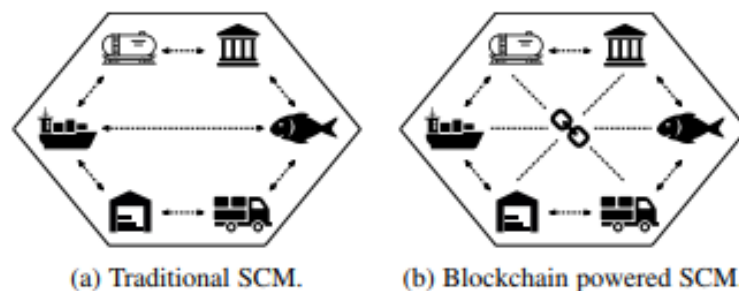


Figure 12: Comparison between a Traditional and a Blockchain powered SCM scheme. (Source: ETH Zurich)⁴³

- **Improving transparency and Traceability:** Monitor provenance and proof of legitimacy and authenticity, not just for business but for the customer too, since he could be able to check expiration dates, if it's ethically sourced or not, if it has been good preserved during the distribution process... WalMart is working on

⁴⁰ DHL and Accenture, 2018, p. 6.

⁴¹ DHL and Accenture, 2018, fols 12–15; Wüst and Gervais, 2017, fols 3–4; Wolfgang Kersten and others, 2017, fols 7–9.

⁴² DHL and Accenture, 2018, p. 13.

⁴³ Wüst and Gervais, 2017, p. 4.

developing a system involving IoT and Blockchain, where if the sensor on the truck detects a temperature increase for an instant, that would be attached to the product information, assuring meat quality. That area of appliance is highly dependent on the development of IoT and sensors.⁴⁴

- **Automating through Smart Contracts:** Current industry estimates indicate that 10% of all freight invoices contain inaccurate data which leads to disputes as well as many other process inefficiencies in the logistics industry. As digitized documents and real-time shipment data become embedded in Blockchain-based systems, this information can be used to enable smart contracts. These contracts can automate commercial processes the moment that agreed conditions are met. Furthermore, Blockchain in combination with the Internet of Things, in the logistics industry will enable even smarter logistics contracts in future. For example, on delivery a connected pallet will be able to automatically transmit confirmation and the time of delivery as well as the condition of the goods to the Blockchain-based system. The system can then automatically verify the delivery, check whether the goods were delivered as per agreed conditions (e.g., temperature, humidity, tilt) and release correct payments to the appropriate parties, greatly increasing efficiency as well as integrity. Blockchain can further be used in the context of IoT to automate machine-to-machine payments (e.g., connected machines negotiating and executing price based on the logistics activities performed).
- **Identify counterfeit products:** By giving a unique digital identity to a product, it's possible to fight the counterfeit problem which assaults many sectors such as the pharmaceutical or the luxury one. That could be done by adding QRs or NFC Chips to every product, containing this codes or chips the information in regard of the unique identity of the asset together with other information. Afterwards, the customer would just need to scan in order to be sure of its precedence and authenticity.

In posterior sections from this thesis, further explanation in regard of the utility which Blockchain can actually provide to the supply chain following the criteria stated in the decision tree from Figure 11 will be given.

⁴⁴ Shaik, 2018.

2.1.6 Real use cases

Despite the technology's novelty, there are many companies who are starting to experiment, develop, try and even to use Blockchain based logistic systems. The majority of this products and services do not cover the whole supply chain but manage small and concrete parts of it. Below, some real use case examples together with an explanation can be found⁴⁵:

- **Power Ledger:** Australian Startup which enables users to sell their surplus of renewable energies to other peers in the network. The Power Ledger system tracks the generation and consumption of all trading participants and settles energy trades on pre-determined terms and conditions in near real time. A user simply receives a registration email from their Application Host, they click on a link which takes them to the Power Ledger platform where they create a user id and password. Once logged in they can see their electricity usage and all their P2P trading transaction details.⁴⁶
- **Renault:** Offers a single source of truth for each vehicle's maintenance data. The data is fully visible to authorized parties such as the owner. Currently, information about customers and their vehicles is spread across multiple information systems maintained by automakers, insurers, repair shops, and more. This new digital car maintenance book, with its open architecture, gathers all important information in one place accessible by the customer. For instance, if an owner wants to sell a vehicle, he/she can make information about the history of the vehicle more transparent by authorizing the potential buyer to access all the data in the digital car maintenance book, creating more trust between the buyer and the seller.⁴⁷
- **Bosch:** Uses Blockchain trying to prevent illegal odometer manipulation. In a digital world with IoT devices, there is a requirement for technology that enables humans to trust a device. In addition, this technology needs to ensure that the information the device provides is correct and trustworthy. Because Blockchain fulfils these requirements, it allows digital contracts to be established between things –which is why it is becoming increasingly popular for IoT use cases. Taking that into consideration, Bosch has developed a certificate based on Blockchain that ensures a car's mileage data is correct. Last year, they started with a proof of concept and connected a real car to the Blockchain. They installed a

⁴⁵ DHL and Accenture, 2018, fols 9–11; Kersten and others, 2017, fols 7–9.

⁴⁶ PowerLedger, 2018.

⁴⁷ Renault, 2017.

connectivity device in the car to read its mileage data. Using the connectivity device, they transmitted then the data to a backend which is connected to a Blockchain. In addition, they developed an app for consumers that enables them to view the mileage history of their car. What's more, users can access an online service to get a digital certificate indicating whether the mileage has been manipulated or not. Their minimal viable product is a complete IoT solution including a connectivity device that is connected to the car, an app for consumers, and a live service to certify the mileage data.⁴⁸

- **VeChain:** Assures the product authenticity through a QR code or a NFC chip. VeChain embeds chips within luxury goods, so brands can monitor their sales channels in real-time to prevent illegal overstock trading. Meanwhile, consumers can verify the authenticity of the luxury products. VeChain puts control back into the hands of brands, making luxury trail transparent, seamless and data-driven. Another Blockchain based use case offered by this company consists on a tracking and authentication platform for wine bottles where data of the wine at every step of the production process is stored on the Blockchain. It also allows logistic providers and distributors to store relevant data before it reaches its destination. This platform brings value and trust, and most importantly stems out illicit activities. Consumer rights are protected simply by scanning a QR Code or NFC Chip which provides authentic and valuable information to the entire timeline starting from the source, storage, and logistics process at the fingertips.⁴⁹
- **Wal-Mart:** Has developed a Blockchain backed automate quality control system. Together with partners, Wal-Mart has conducted a Blockchain test designed to trace the origin and care of food products such as pork from China and mangoes from Mexico. To begin with, this initiative documented the producer of each specified food product so that Wal-Mart can easily address any case of contamination, should this arise. Secondly, the test put mechanisms in place to identify and rectify the improper care of food throughout the journey from farm to store. For example, since meat shipments must not rise above a certain temperature, the test took temperature data from sensors attached to the food products and committed this data to the Blockchain-based system. From there, automated quality assurance processes notified relevant parties in the event of suboptimal transport conditions.⁵⁰

⁴⁸ Stefanie Kowallick, 2017.

⁴⁹ VeChain, 2018.

⁵⁰ DHL and Accenture, 2018, p. 16.

2.2 Internet of Things

As introduced at the beginning of the present thesis, IoT is defined as sensors and actuators connected by networks to computing systems. These systems can monitor or manage the health and actions of connected objects and machines, while the connected sensors can also monitor the natural world, people, and animals.⁵¹ Internet of Things is not a technology, but a concept and a paradigm. It considers an overall presence in the environment of a variety of things that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things in order to create new applications and services to reach common goals. It promises to be able to create a world where the real and the digital spaces are converging to create smart environments which make energy, transport, cities and many other areas more intelligent.⁵²

This concept is extending rapidly and becoming part of a large and growing portion of the world's population daily life. The paradigm is evolving together with the necessity of new applications, visions and the surge of compatible new technologies. Nowadays, it is mostly oriented towards the optimization of the industrial production, being it one of the world's biggest economic factors. IoT is able to help industries as well to cope with the challenges derived from global trends which the sector faces nowadays. The main trends are globalization, rapid technological evolution, dynamization of product life cycles, the aging work force and the shortage of resources. Evident effects of this trends are the acceleration of innovation cycles and the increasing customer demand for high quality and individualized mass produces.⁵³

Within this scenario, IoT is mainly being developed in projects regarding the manufacturing, the supply chain and the supervision of processes. The major question about IoT is in regard the value and the benefit which it can bring to the user and therefore, to the society.⁵⁴

⁵¹ Manyika and others, 2015, p. 9.

⁵² Keyur K Patel and Sunil M Patel, 2016, p. 1.

⁵³ Ovidiu Vermesan and Peter Friess, 2004, p. 154.

⁵⁴ Vermesan and Friess, 2004, p. 21.

2.2.1 Mechanisms of the IoT

The Internet of Things is defined as a mixture of different hardware and software technology's. Without taking into consideration its background –software or hardware- those enabling technologies can be classified in three main groups⁵⁵:

- **Technologies that enable things to acquire contextual information:** The IoT sensing means gathering data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analysed to take specific actions based on required services. The IoT sensors can be wearable sensing devices, smart sensors or actuators.
 - o Wearable sensing devices: Devices whose purpose is to detect events or changes in its environment and send the information to other electronics, frequently a computer processor. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc.
 - o Smart sensors: When a sensor device is packaged together with a CPU, it is called a smart sensor. The sensors really become smart when the tight integration of sensing and processing results in an adaptive sensing system that can react to environmental conditions and consistently deliver useful measurements to a robotic system even under the harshest of the conditions.⁵⁶ They are widely used to make the sensing process more efficient. It's common to use simple sensing devices permanently and given extraordinary situations, they are programmed to trigger more complex sensing systems. For example, air quality sensors may report high risk pollutants, and activate cameras and rich sensing analytics to identify the pollution sources (such as garbage, construction sites, and others).⁵⁷
 - o Actuators: An actuator is a mechanism for turning energy into motion. They work together with smart sensors and sensing devices in order to gather data. For example, in a vehicle where it's desired to measure the

⁵⁵ Patel and Patel, 2016, p. 6123; Ala Al-fuqaha and others, 2015, fols 2348–2350.

⁵⁶ Vladimir Brajović, 2013, p. 156.

⁵⁷ Mahmudur Rahman and others, 2017, p. 2.

air caudal through the engine, the airflow is measured by heating a small element and measuring the rate at which the element is cooling.

- **Technologies that enable things to process contextual information:** Processing units like processors or microcontrollers together with software applications represent the metaphorical brain and the computational ability of the IoT. Various hardware platforms were developed to run IoT applications, such as Arduino, while many software platforms are utilized to provide IoT functionalities. Such as Operating Systems, which are vital since they run for the whole activation time of a device. There are several Real-Time Operating Systems that are good candidates for the development of RTOS-based IoT applications. For instance, Cloud Platforms form another important computational part of the IoT. These platforms provide facilities for things to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data.
- **Technologies to improve security and privacy:** For an IoT environment to be considered secure, there exist a few requirements which are mandatory to be met. Those requirements are:⁵⁸
 - **Confidentiality:** There's a need to assure that only authorized parties are able to access a defined data.
 - **Integrity:** It's necessary to assure the accuracy of the data, by assuring that it's coming from the right sender and that it's not manipulated in any way.
 - **Availability:** Data, services and devices must be reachable and available for the user whenever they are needed or required in a given moment.
 - **Authentication:** It's necessary to be able to identify and authenticate things properly. Identification is crucial for the IoT to name and match services with their demand. Many identification methods are available for the IoT such as electronic product codes (EPC) and ubiquitous codes (uCode).⁵⁹
 - **Policies:** There is a requirement to ensure that data will be managed, protected and transmitted in a safe way through standardized processes and policies. Service Level Agreements (SLAs) must be clearly identified in every service involved.

⁵⁸ Tasneem Yousuf and others, 2015, p. 337.

⁵⁹ Al-fuqaha and others, 2015, p. 2350.

Furthermore, those requirements should be met through lightweight built-in solutions, since the computational and power capabilities of the devices involved in the IoT are limited.

The first two categories can be jointly understood as functional building blocks required building “intelligence” into things, which are indeed the features that differentiate the IoT from the current Internet. The third category is not a functional but rather a de facto requirement, without which the penetration of the IoT would be severely reduced.⁶⁰

In regard of the devices, it’s important to understand that communication is the key for IoT to work. Without communication among the devices it’s not possible to create this interconnected network which has been defined above. The other properties such as sensing, manoeuvring, capturing, storing or processing data will just be necessary if a given specific device requires them (Figure 13).

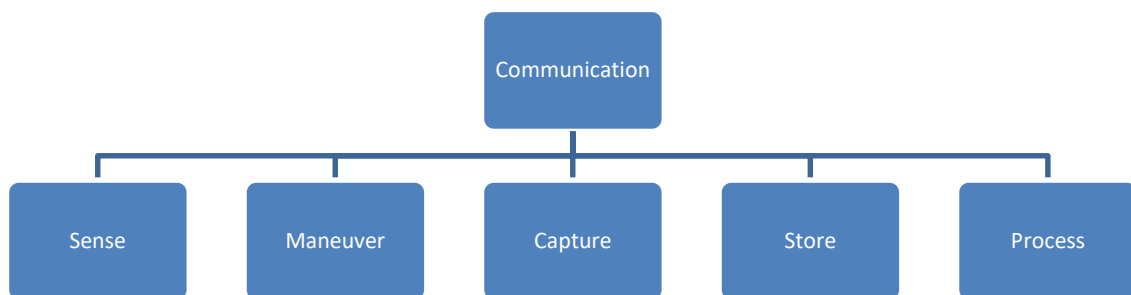


Figure 13: Communication as the key to allow the specific properties from an IoT network of given devices to work.

2.2.1.1 Communication

As said, communication is the corner stone for IoT to function. This communication among devices in a IoT paradigm can occur in three main different ways:

- The first one (Figure 14), would be a device communicating directly with another one (For example, via Bluetooth).



Figure 14: Communication Device-to-device.

⁶⁰ Patel and Patel, 2016, p. 6123.

- The second one (Figure 15), would be devices that communicate to each other through a gateway which communicates with a network using one protocol (For example, IPv4)

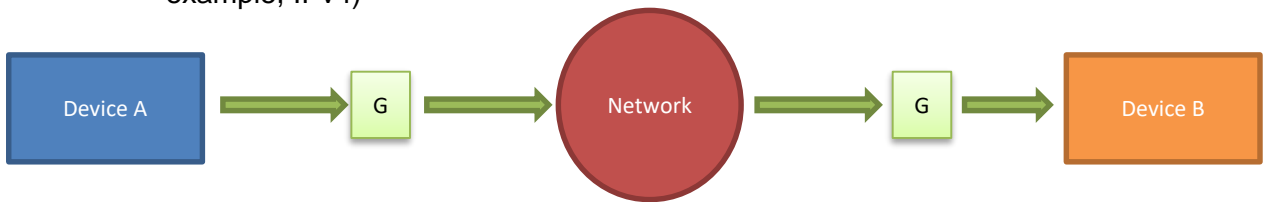


Figure 15: Connection between devices through a Network with an entrance and exit gateway

- Lastly (Figure 16), it's possible to speak about devices which are communicating through a network without requiring a gateway.

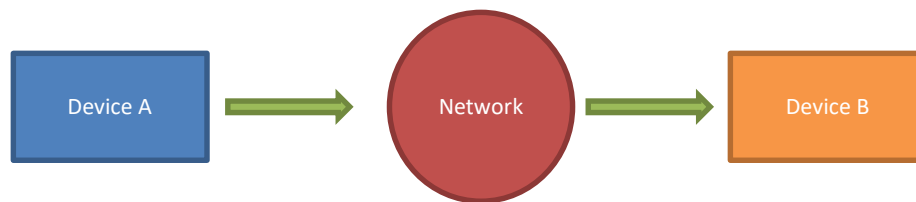


Figure 16: Connection between devices through a Network with no gateway requirements.

2.2.1.2 Main characteristics

The described enabling technologies from the previous chapter aim to give IoT some intrinsic characteristics which makes the paradigm suitable for its purposes and therefore useful. Among the many characteristics which can be found in this concept, it's possible to find below the necessary ones⁶¹:

- **Interconnectivity:** The ability of IoT devices and systems to work together is critical for realizing the full value of IoT applications; without it, most of the potential benefits cannot be realized. Adopting open standards is one way to accomplish interconnectivity together with implementing systems or platforms that enable different IoT systems to communicate with one another.⁶²
- **Things-related services:** IoT requires this kind of services for itself in order to be functional. For example, it should be able to provide privacy protection and consistency between the physical and the digital world. The later, for instance, makes reference to identity-related services.⁶³

⁶¹ Patel and Patel, 2016, p. 6123.

⁶² Manyika and others, 2015, p. 11.

⁶³ Matthew Gigli and Simon Koo., 2011, p. 1.

- **Heterogeneity:** The IoT should be capable of interconnecting billions or trillions of heterogeneous things through the Internet. Those things are considered to be heterogeneous as they are based on different hardware platforms and networks.⁶⁴
- **Dynamic changes:** The state of devices are potentially and constantly changing. For example, they can be connected or disconnected. On the other hand, their context might also be changing too. Examples of that are their current location or the speed at which they are moving. Moreover, the number of devices itself given a network might as well be in constant change. Therefore, the IoT infrastructure needs to be developed in order to be able to withstand and adapt to this dynamic environment.
- **Enormous scale:** The scalability of the IoT makes reference to the capacity to introduce new devices, services and functions for users without negatively affecting the quality of existing services. Adding new operations and supporting new devices is not an easy task especially in the presence of an extremely heterogeneous environment. The IoT applications must be designed from the ground up to enable extensible services and operations.⁶⁵ The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet.
- **Safety:** As explained in the previous section, safety is not defined as a fundamental technological property in order for IoT to exist by itself, but as a required property for IoT to penetrate in our society. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a scalable security paradigm.
- **Connectivity:** Connectivity enables network accessibility and compatibility. Accessibility refers to the capacity of accessing a network while compatibility provides both the capacity to consume and produce data.

Understanding the background technologies as well as the main properties which a proper IoT paradigm should include in order to meet with the actual purposes and expectations it's necessary to observe how does everything get involved and mixed creating the complete concept –the design of IoT's architecture.

⁶⁴ Al-fuqaha and others, 2015, p. 2364.

⁶⁵ Al-fuqaha and others, 2015, p. 2363.

2.2.1.3 Structural architecture

Generally, scientific literature⁶⁶ defines IoT's architecture as a layered structure, even if there isn't any defined as the paradigmatic one and therefore a reference model does not exist. This layered structure divided and named differently depending on the author is based on a bottom to top construction where in the lowest part the perception layer (sensing devices, actuators and smart sensors) can be found. Right above, the network layer is situated in order to work as a medium for data to keep ascending and reach finally the application layer which fulfils the final purpose of the IoT utilisation. The Management Service layer, in charge of the rendering and processing of the information, is sometimes situated inside the application level and sometimes introduced as a different layer level. In this thesis, the second model will be the one used to describe the paradigm because it permits a better dissection and examination of the layers and it gives data managing the importance which it deserves. In the Figure 17 a graphical representation of this layer distribution can be observed, being it a simplification of the one created by the Patel⁶⁷ brothers.

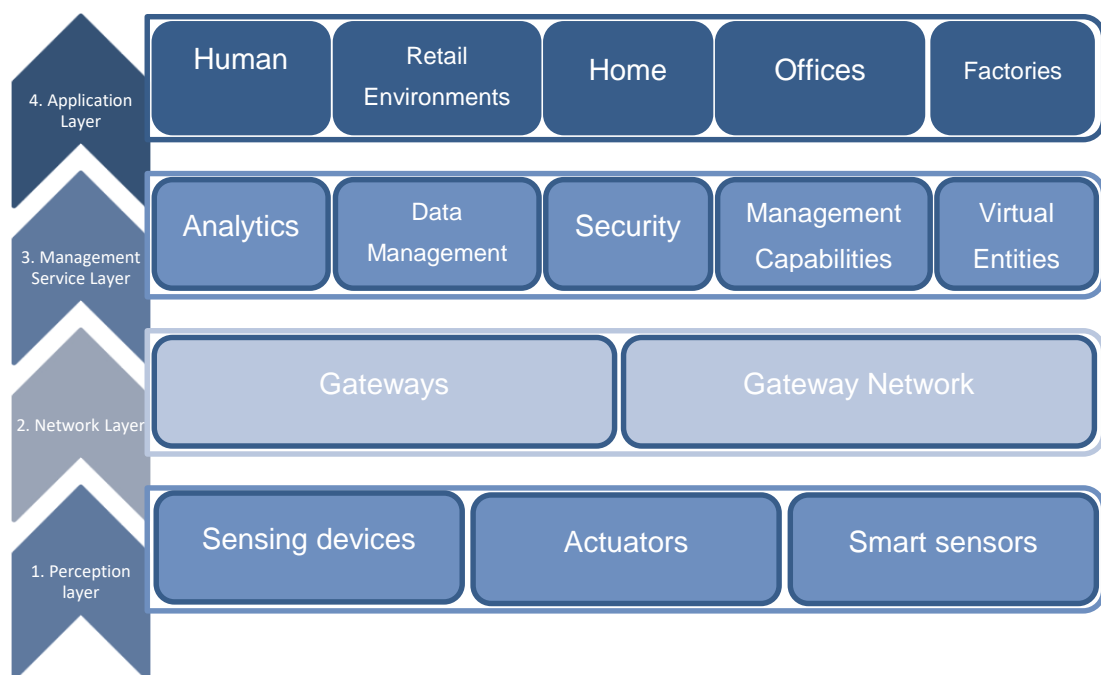


Figure 17: IoT's architecture graphical representation.

- **Perception layer:** This layer level is formed by an integration of sensing devices, actuators and smart sensors which enable the interconnection of the physical and digital worlds. It's in charge of collecting the information taking different

⁶⁶ Al-fuqaha and others, 2015, p. 2349; Patel and Patel, 2016, p. 6126.

⁶⁷ Patel and Patel, 2016, p. 6126.

measurements and, in case of the smart sensors, carrying out small processing and storage labours. Basically, it measures a physical property and converts it into signal that can be understood by an instrument.

- **Network Layer:** The information gathered in the previous layer needs to be transferred to the Service Management layer through secure channels. That information transportation is carried out through networks, usually tied with different protocols which might need -or not- a gateway to be accessed. Those networks can appear as private, public or in-between hybrid models depending on the latency, bandwidth and security requirements.
- **Management Service Layer:** It renders and processes the data through analytics, management systems, security controls, process modelling and management of devices together with their virtual identities. The data which arrives into this layer might follow two different routes afterwards. It can either need to be filtered or redirected to post-processing systems or it might require an immediate response to a given situation. Basically, it entails the logic decisions from the paradigm.
- **Application layer:** As a simplified summarization, the data is collected on the perception layer, transported through the network, processed in the service management level and, finally, it reaches the application layer. This layer provides the desired services, being those high-quality and highly automated ones. It enables concepts such as smart houses or buildings and it permits to optimize business such as transportation, industrial manufacturing or healthcare among others.

2.2.2 Theoretical potential

Almost every big logistic, technological or consulting company has a infographic trying to determine which will be the value of IoT⁶⁸ in a few years, but they mostly appear to be not well grounded. When looking at the predictions that they were making a few years ago about what were they expecting of today's market to be, it's possible to observe that they tended to be bullish and overhyped, as most of them were expecting 50B⁶⁹ devices in 2020 and the status quo is not even close to that number. McKinsey⁷⁰ states that the whole IoT industry will have a 4-11\$BT impact per year, IDC said in 2014 that as of today

⁶⁸ James Macaulay, Lauren Buckalew, and Gina Chung, 2015, p. 5; IDC, 2014; Manyika and others, 2015, p. 7.

⁶⁹ Nordrum, 2016.

⁷⁰ Manyika and others, 2015, p. 7.

we should have 4,6T\$⁷¹ in IoT infrastructure and DHL together with Cisco affirm that it will be around 8T\$⁷² value at some point over the next decade. The numbers seem to more or less converge but the predictions are vague and therefore in this chapter only the technological potential -and not the economic value that it could generate- will be discussed.

2.2.2.1 *Segment potential*

IoT impacts in a different way different market segments. A basic segregation in order to study this different impacts consists in splitting between companies or enterprises, consumers or customers and the government:

- **Impact on companies:** IoT offers two different improvement options for the companies. The first one consists on transforming current business models by making them either more efficient or more effective, while the second one refers to the capacity of unleashing new business models which were not feasible or imaginable before by unlocking new technological possibilities. Therefore, it's possible to affirm that IoT gives companies the possibility of:
 - o Improving their operations.
 - o Redefining their customer relationships.
 - o Creating new revenue streams.
- **Impact on customers:** On the other side of the equation, customers see a quality increase on many of their daily activities since the services which they have access to become more efficient and effective. The three largest benefits can be grouped in:
 - o An overall more convenient lifestyle.
 - o Significant improvements in healthcare.
 - o Increased control and automation over homes and automobiles.
- **Impact on governments:** This promised efficiency improvement generated by the application of the IoT paradigm allows public authorities to evolve towards smart cities. That means that many costly and non-efficient processes could be easily automated in order to reduce the economic and energetic derived impact as well as improving citizen's quality perception. Some examples could be:

⁷¹ IDC, 2014.

⁷² Macaulay, Buckalew, and Chung, 2015, p. 5.

- The automation of the street lighting depending on factors such as the external light levels or the real-time energy price.
- The simplification of traffic monitoring
- The development of intelligent buildings.

2.2.2.2 *Sectorial applications*

Taking into consideration the current state of art for the IoT, as well as the future perspectives, it is possible to split the different applications in a large variety of sectors and situations, permeating into almost all the areas of everyday life of individuals, enterprises and society as a whole. In this chapter the ones with promises of bigger impact⁷³ –both financial and non-financial wise- will be detailed (Figure 18):

- **Human body:** Within the human body it's possible to find two main categories, the first one referring to an improvement on a health level and the second one enabling a productivity increase. This approach won't be used as the majority of IoT applications, where the data follows the path described in section 2.2.1.3 Structural architecture from the Perception Layer until its application. In this case, the sensors will read the data, which after being processed will be displayed to the people, who will use it in order to take decisions.⁷⁴

In the healthcare side, it's possible to observe a wide range of opportunities⁷⁵:

- Patients Surveillance: It permits to monitor the health status of the patients gathering real-time data in hospitals and old people's homes. It also permits early detection of complications as well as to improve the treatment of chronic diseases.
- Medical fridges and quality: Permits a rigorous control of the conditions inside medical fridges as well as the validity of the medicaments inside.
- Dependant people care: Real-time vigilance for elder and dependant people. For example, detection in case of fall and automation of subsequent activities.
- Physical activity and sleep monitoring: Sensors placed across our daily life objects (smartphone, bed...) or implanted which tracks our daily

⁷³ Manyika and others, 2015, p. 3.

⁷⁴ Manyika and others, 2015, p. 8.

⁷⁵ Patel and Patel, 2016, p. 6130; Manyika and others, 2015, fols 37–39.

activity providing the user information in regard of his daily activity, energy consumption, sleeping habits and quality etc.

Regarding the productivity issue, there is a wide range of possible applications as well which are able to track and enhance human performance⁷⁶:

- Augmented reality: It could potentially assist surgeons, mechanics, firefighters etc. as well as other users who have no access to consulting guides in real time. For example, creating augmented reality electronic glasses which display graphic for the worker in order to assist him. It could be used too to train workers for specific and dangerous situations.
 - Pathing: Followed daily routes could be easily tracked and analysed, giving the user the detailed information in regard of it and purposing better and time saving alternatives.
 - Health and safety: In dangerous environments, possible accidents could be predicted and prevented. For example, displaying sounds whenever the worker gets close to a moving machine part or using sensors to detect and advert him of possible radiation or chemicals.
- **Home**: In the household scenario, IoT brings its utility in an energy management, security and automation of domestic processes way. Being the last one, by far, the one which implies larger benefits.⁷⁷
- Information and automation: Refrigerators with LCD screens telling what's inside, information in regard of food which is about to expire, ingredients that you need to buy etc. connected to your Smartphone. Home appliances, such as the washing machine, allowing you to control the laundry remotely or self-cleaning oven's that adjust their temperature based on the food inside.
 - Safety monitoring: Sensors and cameras connected to alarm's and security systems or detection of opened windows and doors at undesired times.
 - Energy and water consumption: Monitoring the energy and water supply consumption together with the current prices, showing the user the patterns and advices about how to save or even automating efficiency process.

⁷⁶ Manyika and others, 2015, fols 46–47.

⁷⁷ Manyika and others, 2015, fols 52–54; Patel and Patel, 2016, p. 6130.

- **Retail environments:** Defined as physical environments which consumers approach in order to purchase a good or a service, could improve the user experience as well as reduce the cost for the supplier.⁷⁸
 - Automated checkout: Could dramatically smooth the checkout process both for the customer and the provider. Nowadays there are some approaches to this field, but with IoT it could be fully autonomous, by scanning the content of shopping items and automatically charging the customer when leaving the store.
 - Layout optimization: By studying the movement and patterns which the shoppers follow, the layout together with the item allocation could be improved.
 - Inventory optimization: The stock management could be leaner, by better understanding the current warehouse capacity and utilization by sensors, and by using predictive algorithms in order to forecast future demand. Further steps could include automated self-replenishment.
- **Offices:** As well as the home section, the main IoT applications related with the office environment are given by the management of energy and security systems.⁷⁹
 - Energy and environment management: The main energy waste activities coming from office facilities are heating, cooling and lighting. Often that's centralized and therefore it's wasting energy in unrequired occasions such as empty rooms. Thanks to IoT, sensors could be able, for example, to detect an empty room in order to close the lights or the air conditioning system.
 - Building security: Pattern-recognition technologies could be added to the traditional monitoring systems –such as cameras- in order to make the process more efficient and less costly. An example would be to just store data or to increase the image quality given certain situations
- **Factories:** A wide variety of processes could be automated in the industrial field, from the manufacturing processes to the inventory management.⁸⁰
 - Maintenance and repair: IoT would permit early predictions on equipment malfunctions while allowing service maintenance to be automatically scheduled and even carried out.

⁷⁸ Manyika and others, 2015, fols 60–62.

⁷⁹ Manyika and others, 2015, fols 63–65.

⁸⁰ In Lee and Kyoochun Lee, 2015, fols 33–34.

- Inventory optimization: The stock management could be leaner, by better understanding the current warehouse capacity and utilization by sensors, and by using predictive algorithms in order to forecast future demand. Further steps could include automated self-replenishment.
- Operations optimization: IoT would make possible real-time adjustments at different points from the production process warranting an uninterrupted flow of finished goods.
- **Worksites**: Including oil and gas exploration and production, mining and construction, these activities are usually carried out in dynamic and dangerous environments. The IoT, in this kind of sectors where industries depend on costly and complex equipment to get the job done, aims to increase productivity by improving the equipment reliability, reducing uncertainty in regard of the environment, protect the asset integrity and manage the processes and the supply chain efficiently.⁸¹
 - Operations optimization: Covering the automation of a variety of processes such as self-driving trucks as well as the improvement of the data management by making it more available and highlighting the key information.
 - Improved equipment maintenance: It involves a condition-based maintenance, by locating sensors in the key spots from the machinery which allows to track its state and performance and therefore being able to carry out preventive maintenance tasks when required.
 - Health and safety: As said above, usually this tasks are carried out in potentially dangerous environments. IoT-based protocols could be built in order to reduce and prevent accidents and injuries. For example, when a heavy machinery detects human presence close to a dangerous spot it should stop its activity.
- **Vehicles**: Including cars, trains, ships and aircraft, IoT aims to locate sensors into the vehicles in order to achieve three things simultaneously: self-driving capacities, condition-based maintenance and behavioural understanding leading to product improvement.⁸²
 - Safety and security: There are many applications coming from IoT in that sense, from predictive collision system to the automation of the braking process.

⁸¹ Manyika and others, 2015, fols 78–80.

⁸² Manyika and others, 2015, fols 82–84; Harvard Business Review, 2014, fols 4-5; Derek O'Halloran and Elena Kvochko, 2015, fols 9–10.

- Condition based maintenance: It's way more cost efficient to carry out preventive condition-based maintenance labours than corrective ones. IoT would permit early predictions on equipment malfunctions while allowing service maintenance to be automatically scheduled.
- New features: Such as self-driving capabilities or behavioural-based insurance tariffs.
- **Cities**: Cities are evolving towards the called “smart” cities where IoT is used to improve the offered services, relieve traffic congestion, improve energy and water efficiency and overall improve the quality of the citizen.⁸³
 - Structural Health: Monitoring of material conditions in all kind of infrastructures allowing a condition-based maintenance.
 - Lighting: Intelligent and light-adaptive lighting.
 - Safety: Digital video monitoring, fire control management, public announcement systems etc.
 - Transportation: Smart roads and highway interconnected with the vehicle helping to decrease accidents and traffic jams among others.
 - Waste management: Detection of rubbish levels in containers in order to make picking-up routes more efficient by allowing the workers to know if the content inside is large enough to be collected or not.
- **Outside**: Makes references to IoT applications which are carried out outdoors between urban environments such as vehicular navigation, container shipping and package delivery.⁸⁴
 - Logistics routing: Real-time IoT data intake allows real-time truck routing, making routes more efficient based on the situation (traffic, delivery spots, oil stations etc...).
 - Tracking goods in transit: Could improve customer satisfaction since he would be aware of the shipment information while improving the container utilisation for the provider.

⁸³ Patel and Patel, 2016, p. 6130.

⁸⁴ Manyika and others, 2015, fols 97–98.

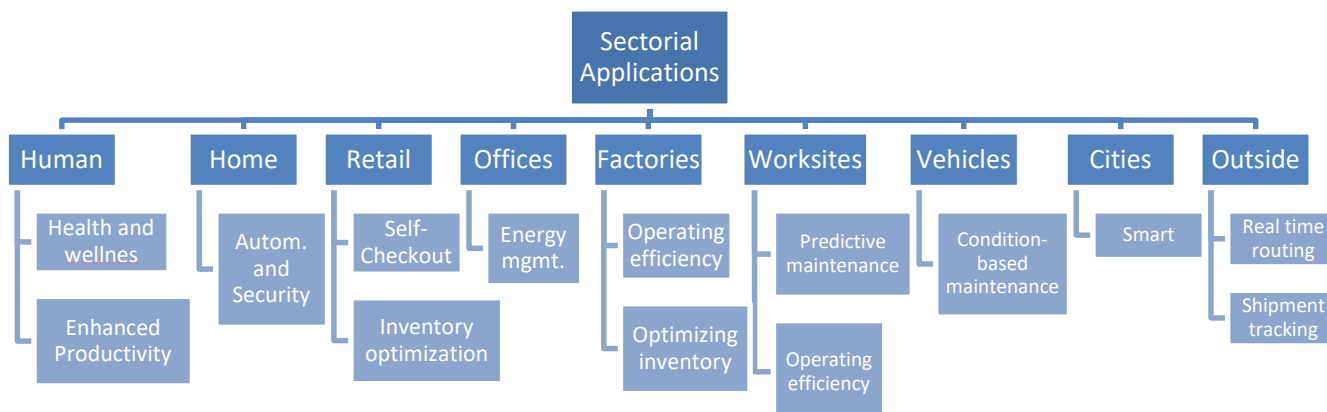


Figure 18: Main IoT Applications divided by sector.

2.2.2.3 Key drivers and Challenges

Nowadays there is a large number of key drivers which the paradigm needs to adopt in order to succeed and penetrate into our society as well as many challenges which need to be surpassed for the same reason. Regarding the key drivers, as IoT is understood as a concept which implies many technologies, improvements in each of this fields would imply an improvement for the paradigm and therefore pushing it forward (Figure 19).

Technology	Future development	Research needs
Hardware Devices	<ul style="list-style-type: none"> - Nanotechnology - Miniaturization of chipsets - Ultra low power circuits 	<ul style="list-style-type: none"> - Low cost modular devices - Autonomous circuits
Sensors	<ul style="list-style-type: none"> - Tiny sensors - Low Power sensors - Wireless sensor networks for sensor connectivity 	<ul style="list-style-type: none"> - Self-powering sensors
Communication Technology	<ul style="list-style-type: none"> - On chip antennas - Wide spectrum protocols - Unified protocols - Multifunctional reconfigurable chips 	<ul style="list-style-type: none"> - Protocols for interoperability - Multi-protocol chips - Gateway convergence - On chip networks
Network Technology	<ul style="list-style-type: none"> - Self-aware and self-organizing networks - Self-learning 	<ul style="list-style-type: none"> - Grid/Cloud network - Software defined networks - Service based network

	- IPv6-enabled scalability	
Software and algorithms	- Goal oriented software - Distributed intelligence - User oriented software	- Context aware software - Evolving software - Self-reusable software - Self-configurable - Self-management
Data and signal processing technology	- Context aware data processing - Cognitive processing and optimization - Complex data analysis - Energy aware data processing	- Common sensor ontology - Distributed energy efficient data processing - Autonomous computing
Discovery and Search Engine technologies	- Automatic route tagging and identification management centres	- Scalable discovery services for connecting things with services
Security and privacy technologies	- User centric context-aware privacy and privacy policies - Privacy aware data processing - Security and privacy profiles selection based on need	- Low cost secure and high performance identification/authentication devices - Decentralized approaches to privacy by information localization

Figure 19: Summarizing the core technologies for IoT which could push it forward and its required scientific developments. (Source⁸⁵: K. Patel, S. Patel)

Nevertheless, there are two laws which are able to explain the current IoT success and the optimistic future predictions:

- **Moore's law:** It observes that over the history of computing hardware, the number of transistors in integrated circuits doubles approximately every two years. This has enabled people to develop more powerful computers on the same sized chip. Intel, a well-known semiconductor chip maker, had during 1971

⁸⁵ Patel and Patel, 2016, p. 6127.

around 2300 transistors on a processor and by 2012 their processors contained 1.4 billion instead.⁸⁶

- **Koomey's law:** It explains that the number of computations per kilowatt-hour roughly doubles every one and a half years. This trend has been remarkably stable since the 1950s (R^2 of over 98%) and has actually been somewhat faster than Moore's law.⁸⁷

Combining these two law interpretations it's easy to say that it's possible to perform the same amount of computations on an increasingly smaller chip, while consuming decreasing amounts of energy. Hence, computations are becoming more energy and space efficient.

On the other hand, in regard of the challenges which the society needs to face in order to embrace and be able to widely adopt IoT as a paradigm, there are many issues to be discussed such as data management or privacy:

- **Data management and mining**⁸⁸: IoT derived sensors are collecting and gathering data constantly. That translates into an immense amount of data which has a huge need for a robust infrastructure if it's desired to be processed and saved. Nowadays few companies own this kind of infrastructures and they are unlikely to invest the required amount of money.
- **Cost versus utility**⁸⁹: The IoT application employs a huge number of sensing and actuating devices, and in consequence its cost and its payback period will be an important factor. For its adoption to grow, the cost of components that are needed to support capabilities such as sensing, tracking and control mechanisms need to be relatively inexpensive in the coming years.
- **Interoperability and standardization**⁹⁰: Different industries today use different standards to support their applications. With numerous sources of data and heterogeneous devices, the use of standard interfaces between these diverse entities becomes important.
- **Privacy**⁹¹: Personal privacy issue (data ownership) is a major concern in employing IoT networks as the connected objects and devices can be easily

⁸⁶ David House, Gordon E Moore, and International Technology Roadmap, 2015, p. 1.

⁸⁷ Jonathan G. Koomey and others, 2011, fols 46–47.

⁸⁸ Lee and Lee, 2015, fols 438–439.

⁸⁹ Patel and Patel, 2016, p. 6129; Sunil Luthra and others, 2018, p. 734.

⁹⁰ Patel and Patel, 2016, p. 6129.

⁹¹ Lee and Lee, 2015, p. 439; Luthra and others, 2018, p. 734.

traced and hacked. As many applications require user's data such as location, health condition or purchasing preferences, protecting privacy is often counter-productive to service quality.

- **Security and chaos**⁹²: Security has a crucial role in successful deployment of any network at any scale. Billions of devices are connected through IoT which calls for the need of efficient security mechanisms that not only helps in protecting the information but also control de derived actions. In a hyper-connected world, an error in one part of a system can cause a chain reaction. Evident examples of that are what could happen in case of technological malfunction in smart home or medical monitoring applications. The risk is elevated and the consequences could be fatal.
- **Talent and infrastructure**⁹³: The IoT application needs a more complex and bigger infrastructure than that which we have nowadays in order to support and manage the high amount of interconnected devices efficiently. This problem affects specially underdeveloped countries.

2.2.3 Possible logistic applications and related use cases

With large and still increasing number of assets being moved, tracked, and stowed by a variety of machines, vehicles and people every day, it is no surprise that logistics and IoT have a clear symbiosis.⁹⁴ Leading companies across multiple industries are already reaping tangible benefits in improving operations, lowering costs, generating revenues and creating competitive advantages. Internet of Things is rearranging entire supply chains from production all the way to consumption.⁹⁵ These benefits extend across the entire logistics value chain, including warehousing operations, freight transportation, and last-mile delivery by enabling operational efficiency, safety and security, customer experience, and new business models among others.⁹⁶ Below its main applications together with related use cases are detailed:

- **Warehousing**: Warehousing operations imply nowadays a source of competitive advantage. Those who are able to perform and carry out this tasks in a faster,

⁹² Lee and Lee, 2015, fols 439–440; Luthra and others, 2018, p. 734.

⁹³ Luthra and others, 2018, p. 735.

⁹⁴ Macaulay, Buckalew, and Chung, 2015, p. 7.

⁹⁵ O'Halloran and Kvochko, 2015, p. 28.

⁹⁶ Macaulay, Buckalew, and Chung, 2015, p. 14.

cost-efficient, and more flexible way have larger chances of being successful. Among the main applications it's possible to distinguish between⁹⁷:

- Smart inventory management: With too much inventory on hand, manufacturers have high carrying costs which prejudices the working capital. On the other hand, too little inventory results in stock-outs. Inventory levels can be fine-tuned using automated shelf replenishment and real-time inventory monitoring through sensors that can track the weight or height of items in inventory, triggering automatic reordering based on specific conditions. Therefore, it's possible to create a permanent regimen where the inventory levels are close to the optimal defined stock.⁹⁸
- Damage detection: Through attached cameras which are able to capture images from pallets and other items. Afterwards those images are processed in order to determine the state of the objects.
- Predictive maintenance: One of the most developed and currently used application of the IoT in Logistics is predictive maintenance and remote asset management, which can reduce equipment failures or unexpected downtime based on the operational data now available. Thames Water, the largest provider of drinking and waste-water services in the UK, is using sensors, analytics and real-time data to anticipate equipment failures and respond more quickly to critical situations, such as leaks or adverse weather events.⁹⁹
- Optimal asset utilization: By connecting machinery and vehicles to a centralized system through a network, IoT enables real time asset monitoring. It's possible to determine when an asset is being over-utilized or when vice versa occurs. Analysis of the data could then identify optimal capacity rates and tasks for the assets. One such innovation is Swisslog's "SmartLIFT" technology. The solution combines forklifts sensors with directional barcodes placed on the ceiling of the warehouse to create an indoor GPS system that provides the forklift driver with accurate location and direction information of pallets.¹⁰⁰

⁹⁷ Macaulay, Buckalew, and Chung, 2015, p. 14.

⁹⁸ Macaulay, Buckalew, and Chung, 2015, p. 16; Manyika and others, 2015, p. 71.

⁹⁹ O'Halloran and Kvochko, 2015, p. 3.

¹⁰⁰ Macaulay, Buckalew, and Chung, 2015, fols 16–17.

Amazon now operates one of the world's largest fleets of industrial robots in its warehouses, where humans and robots work side-by-side, capable of fulfilling orders up to 70% faster than a non-automated warehouse. While robots perform picking and delivery, human workers spend more time on overall process improvements such as directing lower-volume products to be stored in a more remote area.¹⁰¹

- **Freight transportation:** It's a fairly developed application. Therefore, nowadays the purpose is to make it faster, more accurate and predictive, and more secure. Freight and parcel delivery are enabled by IoT technologies which provide them with additional efficiency by enabling new features such as real-time truck routing based on IoT tracking data. The industry carries goods from one link in the supply chain to another—from ports to warehouses, from warehouses to distribution centres, and from distribution centres to retail outlets and consumers. This transportation can be optimized through real-time smart routing of vehicles to avoid congestion.¹⁰²
 - o Location and condition monitoring: IoT provides a new level of transport visibility and security thanks to telematics sensors which transmit data on location, condition (whether any thresholds have been crossed), and if a package has been opened (to detect possible theft).
 - o Fleet management: Sensors can monitor how often a vehicle or other assets are in use. Afterwards the data is transmitted for analysis on optimal utilization. Many logistics vehicles nowadays are already carrying sensors, embedded processors, and wireless connectivity, therefore, the infrastructure is already built-in. For example, sensors that measure the capacity of each load can provide additional insights concerning spare capacities in vehicles on certain routes. IoT could then enable a central system that focuses on identifying spare capacity along fixed routes across all business units.¹⁰³
 - o Safety: Preventing potential collisions and alerting drivers when they need to take a break. For instance, long-distance truck drivers are often on the road for days in hazardous conditions. Cameras in the vehicle can monitor driver fatigue by tracking key indicators such as pupil size and blink frequency.

¹⁰¹ O'Halloran and Kvochko, 2015, p. 21.

¹⁰² Macaulay, Buckalew, and Chung, 2015, fols 18–20.

¹⁰³ Macaulay, Buckalew, and Chung, 2015, p. 20.

For example, for more than a decade, the package delivery/logistics firm UPS has been developing ORION, the On-Road Integrated Optimization and Navigation system, which uses algorithms to help drivers decide the best route to accommodate last-minute changes.¹⁰⁴ Another solution from DHL is the SmartSensor which offers full-condition monitoring. This intelligent sensor can monitor temperature and humidity, while also indicating shock and light events, to ensure integrity during transportation.¹⁰⁵

- **Last-mile Delivery:** It's a high resource consuming labour since it has seen little automation in the last years. Nevertheless, consumer demands become more sophisticated and delivery points continue to multiply. Therefore, logistics providers face new challenges in order to define systems which provide value for the end customer and operational efficiency for themselves. IoT in the last mile aims to connect the logistics provider with the end recipient in a more efficient way.¹⁰⁶
 - o Optimized collection from mail boxes: Through sensors, it's possible to determine if mail boxes have -or not- some content inside and how long has it been there. This information is provided to the logistic operators who are able to optimize the collection routes in real-time avoiding those spots where there is nothing to be picked.
 - o Automatic replenishment: Sensors are able to detect whenever a retailer is low on stock, given an optimal level, and automatically an order is created asking the nearest distribution centre for the defined product. That permits to reduce the lead time while highly decreasing the out-stock possibility.
 - o Optimize the return trip: IoT would need to connect delivery companies together as well as other vehicles and individuals. Then, when a vehicle is returning after delivering a package it exists the possibility of checking if there is another interested party in traveling the same way in order to monetize this way back. In this scenario not only the delivering company would be benefited, but the whole society as many new and cheap transport possibilities could be enabled.

¹⁰⁴ Manyika and others, 2015, p. 95.

¹⁰⁵ Macaulay, Buckalew, and Chung, 2015, p. 19.

¹⁰⁶ Macaulay, Buckalew, and Chung, 2015, fols 21–23.

Walmart was recently granted a patent that aims at improving last mile logistics through connecting delivery drones to the Blockchain. This would enable them to interact autonomously with other parties and – through smart contracts – to pay fees and duties by themselves.¹⁰⁷ Another example of a IoT application in last-mile delivery is carried out by Eliport. Eliport is developing autonomous robots which are able to go from defined distribution warehouses to people's homes. Through a large quantity of sensors and data processing they are able to move through cities as pedestrians, carrying a given packet and delivering it straight inside a building. Another example, Shyp,¹⁰⁸ is developing new ways to send products and to do pick-ups. Consumers simply take a picture of the item they need shipped and enter all delivery information in an app. Then a Shyp employee collects the item for packing and delivery. Through IoT, logistics providers can connect with people or businesses on their delivery route who would like to send things but don't have the time or means to go to a post office.

2.3 Interaction models

In order to study the possibility of synergy among different technologies or the inclusion of a determined technology within a paradigm, it's possible to find many different approaches among the current academic literature. As no proper standardized methodology in order to carry out this procedure has been found, the systematic review focused on covering several technology combination papers from different fields with the aim of extracting and summarizing the different methodologies observed. Based on the effect that one technology has over other technologies growth rate -understanding by positive growth a wider adoption- it's possible to determine three different interaction modes¹⁰⁹:

- **Pure competition:** The technologies have a negative impact over each other's adoption. That implies that there is an inherent substitution risk and one is displacing the other.
- **Symbiosis:** The technologies have a positive impact over each other's adoption.
- **Predator-prey interaction:** where one technology enhances the other's growth rate but the second inhibits the growth rate of the first.

¹⁰⁷ Kersten and others, 2017, p. 10.

¹⁰⁸ Macaulay, Buckalew, and Chung, 2015, p. 23.

¹⁰⁹ James M Utterback and others, 1996, fols 62–63.

As explained before, IoT is considered to be a paradigm with many different physical and digital technologies working together. Given that situation, Blockchain could be, for example, in competition with other data base technologies which currently work within the IoT environment, but by being the purpose of this thesis to study the interaction between Blockchain and IoT as a whole, it's mandatory to observe the first one as a possible enabling technology for the later. It's necessary to understand that Blockchain will work inside IoT and therefore, pure competition or predator-prey interactions are inherently discarded. Hence, if a possible interaction is proved it will be a symbiotic one.

2.3.1 Possible frameworks

For symbiotic technology interactions it's possible to observe three different general qualitative methodology tendencies based on different frameworks -quantitative procedures were discarded due to the lack of access to relevant data-. The utilization of one of those methodologies over the others depends on the desired scope as well as on the prosecuted objectives. The following possibilities are explained assuming that there is a technology or group of technologies A, a technology or group of technologies B and there's a desire to study their symbiotic interaction:

- 1) Use case interaction: To dissect and list all the use cases for A and to study if there's a possible integration of those use cases in B. To dissect and list all the use cases for B and to study if there's a possible integration of those use cases in A.
- 2) Challenge/Use case solution: To dissect and list all the challenges and adoption barriers for A and to study if there's a possible solution provided by B. To dissect and list all the challenges and adoption barriers for B and to study if there's a possible solution provided by A.
- 3) Common goal interaction: To dissect and list all the use cases for A and B and to study if there's a possible integration of those use cases towards a common goal. An example to illustrate this case would be a hybrid data storage system which combines Blockchain as a data base type technology with another digital data base technology. The difference with the both above described frameworks remains in this one starting by the goal which is pursued and then studying how the use cases from A and B could be combined to achieve it, while for the previous methodologies the starting point is always the use case or the challenge from the technology.

2.3.2 Framework evaluation and selection

Given the three general frameworks proposed on the previous chapter, an analysis detailing the benefits and impediments for each in regard of the prosecution of the objectives of this thesis is carried out.

2.3.2.1 *Use case interaction*

One of the biggest adoption barriers both for IoT and Blockchain is the uncertainty about their value propositions since it's not clear how can those concepts be applied to current business models in order to improve them or even to create new revenue streams. When carrying out a systematic review on the current literature regarding the use of Blockchain as an enabling technology for IoT, it's possible to observe that the common procedure is to develop a use case interaction analysis.¹¹⁰ However, this procedure which is extremely valid to approach the theoretical potential created by the combination of technologies, gives little insight in regard of actual applications with a clear purpose which could help eliminate their shared immediate adoption barrier –the uncertainty about their value propositions-. This outcome vagueness is mainly explained by two reasons:

- 1) There is no explanation about the real utility which the defined Blockchain use case within the IoT entails. Therefore, it's not clear who could get benefited from it or where and when could it be applied. As an example to better illustrate that, Blockchain could indeed provide a solution for IoT systems in order to create a decentralized environment, but maybe there is no requirement for that decentralization at all.
- 2) There is no proper comparison between Blockchain and other technologies which are able to provide the same utility. Maybe Blockchain is indeed able to contribute with a real use case, but another technology provides it as well in a faster, cheaper or more efficient way.

2.3.2.2 *Challenge/Use case solution*

Given the fact that the vast majority of nowadays literature proceeds with the above explained approach and the flaws that it entails, the analysis carried out on this thesis is done in the opposite direction. The IoT challenges defined on the chapter 2.2.2.3 Key

¹¹⁰ Marco Conoscenti, Antonio Vetro, and Juan Carlos De Martin, 2016, p. 2; Shaik, 2018.

drivers and Challenges are further detailed and for each of them a deep analysis regarding how could Blockchain mechanisms improve, alleviate or even solve them is carried out. It's expected that this approach will help to understand the actual possibilities which this technological interaction entails, providing with a pragmatic insight on the issue and trying to map the real value and application opportunities which can actually be useful below the theoretical potential. Nevertheless, this perspective offers as main incompleteness issue the lack of long term vision as the challenges that require to be solved are the ones which IoT is facing nowadays and it doesn't take into consideration future developments.

2.3.2.3 Common goal interaction

Since this thesis puts special emphasis on the logistic applications, it could make sense to start by defining which goals are desired to be achieved on the logistic sector and then study how IoT and Blockchain could work together in order to accomplish them. However, logistics cover a wide variety of sectors with almost endless particularities. Therefore, it would be close to infeasible to develop a complete review in order to summarize all the improvement possibilities and a lot of resources would be required afterwards to carry out a proper analysis for each of them.

2.3.3 Specific model development

Within the selected general framework detailed on the previous section –to match the challenges to be faced by one technology with the use cases provided by the other technology-, a standardized protocol to study the application of Blockchain in IoT's detected adoption barriers has been developed. It consists on a systematic approach which allows to analyse the interaction in a structured manner and it's shaped as it can be observed below:

- 1) To dissect the generic IoT challenges into elemental premises in order to facilitate its posterior analysis.
- 2) To dissect the generic Blockchain applications (section 2.1.2 Theoretical Potential) into defined use cases in order to facilitate its posterior analysis.
- 3) To contrast all the found elemental challenges with the defined use cases in order to determine if Blockchain is able to provide a solution for IoT.

- 4) Given a match between a IoT challenge and a determined Blockchain application it's necessary to carry out an examination detailing why Blockchain is -or is not- better suited than other given technologies.
- 5) Given a determined Blockchain application which is able to solve a defined IoT elemental challenge more efficiently than –or with some benefits over- any other technology, a user perspective will be adopted and an analysis to define if the logistic sector could benefit from it will be made.

As stated before, this protocol has a relative narrow scope since it does not include how the further development of other technologies could influence the possible interaction between Blockchain and IoT, but it provides a robust methodology to study if there's an actual combination synergy which can lead to a real value-adding scenario.

3. Methodology

This thesis aims to determine the possible interaction mechanisms and outcomes of combining Blockchain together with IoT with a special emphasis on the logistics branch. In order to provide an answer to the topic, a systematic data review has been conducted by researching across the latest scientific literature found on Blockchain and IoT topics separately, as well as on models to combine them together. In regard of Blockchain and IoT, the systematic review focuses on summarizing relevant information about them, listing its properties, theoretical potential, possible logistic-oriented applications and use case examples. In occasions, a semi-systematic web search to obtain concrete information was included on the process. For the possible combination methodologies, a review among several academic papers studying the interaction between two or more technologies was carried out.

On the previous sections, IoT has been defined as a paradigm which entails many enabling technologies as well as many flaws. Taking that into consideration and in order to proceed with the systematic review three research questions were formulated:

- 1) Which is the state of the art for IoT and Blockchain?
- 2) Which flaws and improvement areas does IoT possess?
- 3) Are there any Blockchain mechanisms and use cases applicable to those scenarios?

Given the case where the second question turns out to be affirmative, a third one is proposed:

- 4) Have those use cases any utility for the logistic sector?

The first research question aims to give a context to the thesis by explaining the mechanisms of the entailed technologies as well as other relevant data such as their theoretical potential and real use cases. The second and third questions are formulated in order to study how possibly could Blockchain be an enabling technology for IoT and finally, the last question studies the possibility of using the previous applications within the logistic sector.

3.1 Inclusion criteria

In regard of the technological backgrounds and theoretical potential, the strings “Blockchain” and “Internet of Things” were used to search mainly in Google Scholar and IEEE. For the applications and use cases, the gathered data was obtained as well reviewing documents from reputed technological consulting and logistics companies such as McKinsey, Deloitte or DHL. Lastly, the interaction study methodologies have been extracted exclusively from academic papers using a large amount of different strings. In order to select the most relevant papers to fully analyse them, a first approach was carried out observing the titles and a second one reviewing the abstracts. Overall, the three requirements expected to be met by the literature included on the systematic review are:

- Academic paper or well-known technological company document as sources.
- The content is relevant to answer the research questions directly (e.g. Blockchain mechanisms) or indirectly (e.g. Centralized database properties).
- It is written in English.
- It provides with insights about non-related cryptocurrency issues.

3.1.1 Flaws and limitations over the inclusion criteria

There is a large available literature regarding Blockchain and IoT with endless applications for both concepts in several specific areas. Those concrete applications have been summarized in larger application groups in order to study their possibilities within the logistic sector afterwards. However, as being part of relatively novel and emerging technologies, new applications for Blockchain and IoT are being proposed constantly and therefore it exists the risk of non-considered applications. Furthermore, technological consulting and logistics companies have a clear selling interest on the issue. Given that reason, they have carried out several researches and quantitative analysis on the topic, but at the same time a biased perspective is almost inherent to those papers. Although the documents have been analysed with a critical vision the extracted information still entails a capability overestimation possibility.

3.2 Model application

In this chapter, the procedure created on the section 2.3.3 Specific model is applied step by step.

3.2.1 IoT elemental challenges

As stated previously, the main challenges and adoption barriers which IoT is facing nowadays are: (1) The lack of data management and mining capabilities, (2) Uncertainty about the cost versus utility ratio, (3) Lack of interoperability and standardization among the different physical devices and digital services, (4) Privacy concerns, (5) Security concerns and (6) Lack of talent and infrastructure. In order to further study those issues, each one is dissected into fundamental challenges in the table below (Figure 20).

Major challenge	Elemental issue	Description
(1) Lack of data management capabilities	(a) Collection and cleaning	When data is collected from conventional sensors, it may be noisy, incomplete, or may require probabilistic uncertain modelling. ¹¹¹
	(b) Data management	Sensor networks provide the challenge of too much data, too little inter-operability and also too little knowledge about the ability to use the different resources which are available in real time. ¹¹²
	(c) Mining and processing	The large volumes of sensor data necessitate the design of efficient one-pass algorithms which require at most one scan of the data. ¹¹³
(2) Uncertainty about the cost versus utility ratio	(a) Lack of precedents	Few companies have achieved to proof that building up a IoT complex system is paying off in the long term.
	(b) Unclear value	There is few evidence about how, where and when should IoT systems be deployed in order to improve a business model or a process.
(3) Lack of interoperability	(a) Standardization	Standardized resource descriptions are critical to enable interoperability of the heterogeneous resources available through the web of things. ¹¹⁴
	(b) Physical heterogeneity	The objects in the internet of things, are heterogeneous, and may not be naturally available in a sufficiently descriptive way to be searchable, unless an effort is made

¹¹¹ Aggarwal Charu C, 2013, p. 396.

¹¹² Charu C, 2013, p. 398.

¹¹³ Charu C, 2013, p. 4.

¹¹⁴ Charu C, 2013, p. 388.

		to create standardized descriptions of these objects in terms of their properties. ¹¹⁵
(4) Privacy concerns	(c) Digital heterogeneity	The underlying data from different resources are extremely heterogeneous, can be very noisy, and are usually very largescale and distributed. ¹¹⁶
	(a) Privacy in data collection	Once a smart sensor is carried by a user on their person the EPC –Electronic Product Code- becomes a unique identifier for that person. The information about object movement can be used either to track the whereabouts of the person, or even for corporate espionage in a product supply chain. ¹¹⁷
	(b) Privacy in data transmission	The gathered data needs to be transmitted between different entities. Therefore, the ability to provide privacy during the data transmission and sharing process is critical. ¹¹⁸
(5) Security concerns	(a) Data integrity	It's necessary to assure the accuracy and consistency of the gathered data over its entire life-cycle. It aims to prevent unintentional changes to information. ¹¹⁹ It covers object identification, authentication and authorization. Complete, consistent and accurate data should be attributable, legible, contemporaneously recorded, original and accurate. ¹²⁰
	(b) Lightweight protocols	In IoT, there are various resource-constrained devices such as sensor nodes, smart devices, and wearable devices, which only have limited computing power and battery capacity. Although many proposed cryptosystems and security protocols are considered secure and robust, they may not be suitable for the IoT system magnitude. ¹²¹

¹¹⁵ Charu C, 2013, p. 396.

¹¹⁶ Charu C, 2013, p. 395.

¹¹⁷ Charu C, 2013, fols 415–416.

¹¹⁸ Charu C, 2013, p. 417.

¹¹⁹ Efrim Boritz, 2003, p. 4.

¹²⁰ FDA, 2016, p. 2.

¹²¹ Zhi Kai Zhang and others, 2014, p. 2.

(6) Lack of talent and infrastructure	(c) Software vulnerability	During the development stage of a piece of software, programming bugs produced by developers are unavoidable. Bugs that result in security incidents are known as software vulnerabilities. Software vulnerabilities can lead to a number of backdoor problems. ¹²²
	(a) Formation	The design, utilization and maintenance involves a large sum of different technologies which need to be addressed by highly qualified professionals.
	(b) Infrastructure	A IoT environment requires a large amount of physical devices –such as sensors- as well as enabling digital technologies. To meet all this requisites it's just on the hands of few parties and without providing an end-to-end solution the application benefit loses its entire value in many cases.

Figure 20: IoT major challenges and adoption barriers dissected into elemental issues.

3.2.2 Blockchain basic use cases

On the section 2.1.2 Theoretical Potential the three main Blockchain applications are defined as (1) Storage of digital records, (2) Exchange of digital assets and (3) Recordation and execution of Smart Contracts. Following the given methodology, those general applications are dissected into basic use cases (Figure 21).

Major Application	Basic use case
(1) Storage of digital records	(a) Eliminate single point of failure
	(b) Tamper-proof log of events
	(c) Data transparency
	(d) Shared storage unused capacity
	(e) Unique digital identity
	(f) Management of access policies
(2) Exchange of digital assets	(a) Eliminate necessity of a TTP

¹²² Zhang and others, 2014, p. 2.

(3) Recordation and execution of Smart Contracts

- (a) Contracts compliance
- (b) Automated response

Figure 21: Blockchain basic use case dissection

3.2.3 IoT Challenge Blockchain use cases match

Given the described elemental IoT challenges as well as the Blockchain basic use cases, an analysis is carried out in this section to study their possible combination. As explained on the model definition, this section won't include further detail on the benefits which every interaction entails or its possible applications as it consists only on a first approach which determines if there exists an interaction possibility. On the Figure 22 the matching results can be observed.

IoT challenge/Blockchain use case		Eliminate single point of failure	Tamper-proof log of the events	Data transparency	Shared storage unused capacity	Unique digital identity	Management of access policies	Eliminate necessity of a TTP	Process compliance	Automated response
Major challenge	Elemental issue									
(1) Lack of data management capabilities	(a) Collection and cleaning									
	(b) Data management		X		X		X	X	X	X
	(c) Mining and processing									
(2) Cost versus utility ratio	(a) Lack of precedents									
	(b) Unclear value									
(3) Lack of interoperability	(a) Standardized environment									
	(b) Physical heterogeneity									
	(c) Digital heterogeneity									
(4) Privacy concerns	(a) Privacy in data collection									

	(b) Privacy in data transmission	X							X	X	X
(5) Security concerns	(a) Data integrity	X	X	X		X	X	X			
	(b) Lightweight protocols										
	(c) Software vulnerability	X									
(6) Lack of talent and infrastructure	(a) Formation										
	(b) Infrastructure										

Figure 22: Matching IoT correct challenges with Blockchain use cases.

The explanation of the results summarized on the above figure is divided by IoT major challenges on the following sections.

3.2.3.1 Lack of data management capabilities

- a. **Collection and cleaning:** The cleaning is usually performed at data collection time, and it is often embedded in the middleware which interfaces with the sensors. Therefore, the collection and cleaning issues are normally analysed in the context of the physical devices. Blockchain has no use on improving those devices and does not take part on the data flow structure until the storage and management time. Hence, it has no impact on this challenge.
- b. **Data management:** Data management, including all the processes between the collection and the processing, is one of the IoT challenges where more Blockchain applications can be found.
 1. Tamper-proof log of the events: Blockchain mechanisms are capable of assuring that new entries are always appended as a new block to the last block in the tree. Furthermore, for transactional systems (like currencies), once a record is included, it cannot be changed -instead, changes to the transaction are represented as new record entries in the log, providing a complete audit trail of a transaction-. Therefore, within the data management, this tamper-proof log of the events could improve auditing and reduce network packet size.¹²³

¹²³ Charu C, 2013, p. 376.

2. Shared storage unused capacity: Blockchain can work as a bridge between those who are looking to store data and providers willing to store the data for them. This works essentially by sharing a file across a peer-to-peer network where a file is encrypted and then it gets sent to individual computers in the network. Data is broken into shards and Blockchain protocols have enabled users to monetise unused storage with few barriers to entry. That could make the storage of information more efficient and reduce costs.¹²⁴
 3. Management of access policies: Digital signatures can represent the access right or the entitlement defined by the creator of the transaction to its receiver in order to access a specific resource identified by its address.¹²⁵ Therefore, Blockchain inherently provides a robust access management capability: every user poses a unique private key with defined reading and writing rights.
 4. Eliminate necessity of a TTP: The decentralized environment which Blockchain offers, and therefore the elimination of a central party is usually promoted as a privacy and security boosting capability. Nevertheless, removing that trusted party removes one step in the data sharing flow chart allowing peers to interact directly with each other.
 5. Contracts compliance: Blockchain smart contracts permit to track processes against law regulations or agreements between two or more companies engaged in a partnership with pre-defined rules.¹²⁶ That can provide autonomy to the data management since it could remove the requirement of human intervention and speed up bureaucratic lead times.
 6. Automated response: Enabling the automated execution of specified actions based on contractual conditions as validated by all parties. Basically it would be possible to auto-execute recurring business transactions and help to reduce contractual defaults.
- c. Mining and processing**: This IoT challenge is related with the large amount of data collected by sensors and the necessity of one-pass efficient algorithms to process it. Therefore, Blockchain is not able to provide with a solution for that issue.

¹²⁴ Ajay Kumar Shrestha and Julita Vassileva, 2016, fols 4–6.

¹²⁵ Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman, 2016, p. 8.

¹²⁶ Conoscenti, Vetro, and De Martin, 2016, p. 3.

3.2.3.2 *Cost versus utility ratio*

- a. **Lack of precedents:** There is few evidence about large IoT systems which can provide with a significant benefit to the user. Adding Blockchain to the equation brings even more uncertainty and therefore, it could be considered as a drawback in this scenario.
- b. **Unclear value:** Blockchain use cases have nowadays per se an unclear value proposition challenge. Therefore, as well as with the previous item, the inclusion of this technology in the IoT could be considered as drawback and in any case solves the issue.

3.2.3.3 *Lack of interoperability*

- a. **Standardization:** There is few standardizations among industry players in order to homogenize the Blockchain environment. In fact, there's a need to build uniform standards and protocols, rather than develop internal versions to embrace a wider adoption. Hence, Blockchain won't contribute positively to a more standardized system within the IoT.
- b. **Physical heterogeneity:** That heterogeneity refers mainly to the sensors and actuators. Therefore, it's analysed in the context of the physical devices and Blockchain has no use on improving this issue.
- c. **Digital heterogeneity:** Data integration involves synchronizing huge quantities of variable, heterogeneous data that vary in format. Blockchain, as a data base, does not directly help to homogenise the environment and therefore, this challenge interaction won't be further analysed. Nevertheless, the major problem associated with digital heterogeneity is not the management itself, but the lack of mechanisms to do it on a private and secure way. In that sense, Blockchain is indeed able to provide with solutions and the analysis will be carried out in the privacy and security sections.

3.2.3.4 *Privacy concerns*

- a. **Privacy in data collection:** Privacy issues at data collection are related with the middleware which interfaces with the sensors. Therefore, those issues are normally analysed in the context of the physical devices. Blockchain has no use

on improving those devices and does not take part on the data flow structure until the storage and management time. Hence, it has no impact on this challenge.

b. Privacy in data transmission: There are four Blockchain use cases which are able to improve privacy in data sharing processes. Two of them are related with the inherent decentralization characteristics which the technology offers and the remaining two refer to the automation of processes reducing the required human interaction.

1. Eliminate single point of failure: Sensitive data produced and exchanged among IoT devices is stored in Blockchain, whose peer-to-peer nature could ensure the absence of single points of failure.¹²⁷ By being the data scattered into shards across the peers from a decentralized network accessible just for those who own the right private key, it removes the possibility of a malfunction or a hacking attack towards a given centralized entity which endangers the stored information.
2. Eliminate necessity of a TTP: Blockchain decentralized nature removes the necessity of a TTP with full capacities to control the data as a whole. Therefore, privacy concerns regarding deliberated -or not- data-endangering activities carried out by an entity are inherently discarded.
3. Contracts compliance: Privacy preferences enable users to specify which information can be provided to whom in different contexts.¹²⁸ Therefore, reading rights can be attributed exclusively to defined parties or even eliminate the necessity of human interaction during many activities.
4. Automated response: The previous point, contracts compliance, explains how the Blockchain alone, thanks to the Smart Contracts, is able to contrast the data with some given pre-defined rules in order to prove its validity. Smart contract's utility does not end here, since they are able to generate automated responses as well. That implies that given some pre-defined rules and a data input, the Blockchain alone can verify if a transaction meets the requirements to execute an automated action. Hence, there's no need for the data to be read by a human or to leave Blockchain's mechanisms at any point during the whole data management flow reducing privacy uncertainty.

¹²⁷ Conoscenti, Vetro, and De Martin, 2016, p. 1.

¹²⁸ Charu C, 2013, p. 418.

- a. Data integrity:** Blockchain mechanisms provide a solution to assure accuracy and consistency within the data that is managed and covering at the same time object identification, authentication and authorization.
1. Eliminate single point of failure: Sensitive data produced and exchanged among IoT devices is stored in Blockchain, whose peer-to-peer nature could ensure the absence of single points of failure.¹²⁹ By being the data scattered into shards across the peers from a decentralized network accessible just for those who own the right private key and in any case editable, it removes the possibility of unintentional changes due to a centralized authority.
 2. Tamper-proof log of the events: Blockchains are not editable, since changes coming from new transactions are added as new blocks. That assures an unmodifiable and chronological track of the events which improves the reliability of the data over its entire cycle.
 3. Data transparency: The transparency of an open Blockchain stems from the fact that the transactions of each public address are open to viewing. That means that other peers can check the transaction log and it facilitates the data integrity audit.
 4. Unique digital identity: Assets which can be uniquely identified can be registered in the Blockchain. This can be used to verify ownership of an asset and also trace the transaction history. Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in Blockchain and the ownership, transaction history can be validated by anyone.¹³⁰
 5. Management of access policies: The permits of the different parties within a Blockchain are settled with some pre-arranged rules. Therefore, only the owner of a private key is able to carry out a defined action. As every action is attached with the actor's unique digital signature it assures that every observation or recordation will be attributable to someone.
 6. Eliminate necessity of a TTP: Since there is no requirement for a centralized party with a defined power over the data, the inherent risk of undesired modifications disappears.

¹²⁹ Conoscenti, Vetro, and De Martin, 2016, p. 1.

¹³⁰ Michael Crosby and Pattanayak Pradan, 2016, p. 14.

- b. Lightweight protocols:** Blockchains provide more security features but suffer high computational overhead. Therefore, Blockchain is not a good overall security solution as a lightweight protocol. However, public-key cryptosystems are often desirable when data integrity and authenticity are needed and given an elevate security requirement Blockchain could be able to offer the desired security level in a less-consuming way than other commonly used technologies.
- c. Software vulnerability:** Blockchain does not eliminate the possibility of coding bugs which can eventually lead to a malicious backdoor. However, in a scenario where the programming is robust, it enhances security by removing the single point of failure issue.
 1. Eliminate single point of failure: Blockchain makes the possibility of hackers breaking into the network unfeasibly hard. The data is decentralized, encrypted, and cross-checked by the whole network. Once a record is on the ledger it's almost impossible to alter or remove without it being noticed and invalidating the signature.

3.2.3.6 *Lack of talent and infrastructure*

- a. Formation:** In many cases, to find experts in IoT field is complicated, and therefore not easy to create a solid team able to handle a complex system properly. Blockchain, on the other hand, as a new technology is lacking experts in the field as well. Therefore, integrating Blockchain within an IoT system will increase its technical difficulty as well as the difficulty of finding professionals in the matter. Hence, Blockchain won't provide with a solution for that challenge but quite the opposite.
- b. Infrastructure:** Blockchain is not able to provide a solution within the physical infrastructure and neither one for the digital. In fact, the problem entailed in IoT as a lack of infrastructure -in both senses- that precludes an end-to-end connection affects Blockchain as well by compromising the data that is added to it. Even if this data base type assures immutability, that's of no use if the collected data was manipulated before reaching it.

3.2.4 *Advantages versus centralized databases*

Once carried out the first approach matching those Blockchain functionalities which could aim to solve one or more challenges entailed by IoT as of today, it's necessary to

evaluate the real utility of this interactions by comparing them with other database possibilities. Below, a table including only the found matches is attached.

IoT challenge/Blockchain use case		Eliminate single point of failure	Tamper-proof log of the events	Data transparency	Shared storage unused capacity	Unique digital identity	Management of access policies	Eliminate necessity of a TTP	Process compliance	Automated response
Major challenge	Elemental issue									
(1) Lack of data manag. cap.	(b) Data management		X		X		X	X	X	X
(4) Privacy concerns	(b) Privacy in data transmission	X						X	X	X
(5) Security concerns	(a) Data integrity	X	X	X		X	X	X		
	(c) Software vulnerability	X								

Figure 23: Found matches between IoT challenges and Blockchain use cases.

From the six defined main challenges for IoT adoption, it has been found that Blockchain is able to offer at least partial solutions to three of them: (1) Lack of data management capabilities, (4) Privacy concerns and (5) Security concerns. The elemental issues which could be improved by Blockchain are:

- Improving the data management capabilities
- Increasing the privacy during the data transmission
- Assuring data integrity during the data life-cycle in which the Blockchain is involved.
- Reduce the Software vulnerability possibility.

On the section 2.1.4 Blockchain’s utility, a brief insight based on Wüst and Gervais -from ETH Zurich- first structured methodology¹³¹ is given on the basic differences between Blockchain and centralized databases as well as a criteria to discard those scenarios where Blockchain makes no sense. It’s important to remember that there is no evidence so far where a Blockchain is able to improve the throughput and latency in comparison

¹³¹ Wüst and Gervais, 2017, p. 7.

with a centralized database.¹³² In order to exemplify that, it was determined¹³³ that the cost for business process execution on Ethereum Blockchain –the second largest cryptocurrency by capitalization- are orders of magnitude higher than those achieved through Amazon SWF (0,36\$ vs 0,001\$ per process instance). Those numbers are hardly extrapolable to the overall Blockchain cost efficiency versus the one provided by traditional databases, but it helps to illustrate that so far there are no proven scenarios where Blockchain increases efficiency in those terms. That means that Blockchain and traditional databases are not strictly competing as technologies, since they should be applied on different scenarios. If there are no multiple writers, it exists the possibility of using an always online TTP or all the writers are known and trusted, Blockchain makes no sense since it adds no benefits in terms of data management, security or privacy and at the same time it reduces its efficiency.

Understanding that, it's clear that there is no use in comparing Blockchain with other traditional database technologies on an overall level. The key point relies on understanding their strengths and weaknesses while analysing carefully the scenario in order to choose the best suited option. The three possible scenarios are:

- 1) “There aren't multiple writers” OR “It's possible to use an always online TTP” OR “All witters are known and trusted”
- 2) “There are multiple writers” AND “It's not possible to use an always online TTP” AND “Not all writers are known”
- 3) “There are multiple writers” AND “It's not possible to use an always online TTP” AND “All writers are known” AND “Not all writers are trusted”

In the first option a Blockchain would be of no use, while on the second and third, it might be better suited than centralized databases. However, those theoretical scenarios where Blockchain could be a value-adding technology are hard to be encountered on the real world. On the next section, they are further detailed, aiming to match them with existing situations on the logistic environment.

¹³² Wüst and Gervais, 2017, p. 3.

¹³³ Paul Rimba and others, 2017, fols 2–4.

3.2.5 Use scope: Logistics

As explained on the theoretical background section, IoT as a paradigm has been growing in adoption and spreading across different sectors, including the logistics one. There are many use cases which are able to improve the supply chain efficiency in different areas, but despite Blockchain promises to be able to push even forward those IoT benefits on the supply chain management, there's few legit evidence of proven cases.

Following the given methodology to determine if a Blockchain is well suited or no, it's possible to prove that there are real scenarios on the supply chain management where it would make sense.

- 1) There is an obvious need to store data
- 2) The supply chain is almost always formed by different parties with a need to interact.
- 3) There are scenarios where there's a desire of removing a TTP –either because it makes the process more complicated or because there's no possibility of finding one-.
- 4) All the parties which might have writing powers are probably known –therefore making the possibility of a permissionless Blockchain highly unlikely- but not that probably trusted.

A permissionless Blockchain makes sense when there are a lot of writers which are not known. This scenario is given within peer-to-peer or consumer-to-consumer (C2C) cases and are solved through the utilization of a cryptocurrency token which enables the exchange of value among the participants. However, this thesis aims to find out Blockchain use cases which could be applied in an interconnection with IoT on the logistic sector. Therefore, it has a business scope (B2B or B2C) and cryptocurrency-related options are not included.

On the other hand, when all the writers are known but not trusted, permissioned Blockchains seem to be applicable. To illustrate that, it's taken as an example a supply chain with five different mutually untrusted parties with defined functions involved who can't agree on a TTP: (1) raw material provider, (2) manufacturer, (3) warehouse, (4) distributor and (5) retailer. A permissioned Blockchain would allow to set pre-defined rules and give each of them specific rights (e.g. through a smart contract, the manufacturer pays the raw material provided once the freight is received but if the quality

of the product turns out to not fit within the pre-defined rules, the paid amount is automatically sent back from the provider to the manufacturer).

Reached this point, it seems coherent to adopt a Blockchain solution for scenarios matching the requirements described on the above example. However, there's a problem within the Blockchain which affects other use cases -such as Bitcoin- as well and results to be fatal for its application on the IoT paradigm and even more pronounced when applied to the supply chain: the oracle problem.

3.2.5.1 *The oracle problem*

The oracle problem refers to the inability which Blockchain entails to interact with the outside world.¹³⁴ That problem is already partially limiting for cryptocurrencies like Bitcoin or Ethereum which only operate with data that is already on the Blockchain (e.g. all the Bitcoin tokens are not backed by any real world asset and they were created together with their Blockchain; they are not a digital representation of any physical thing) but it's extremely limiting for environments with an inherent requirement of interaction with the real world –which is the case of IoT and the logistic sector-. Following the previous example, it's said that if the raw materials received do not match a quality standard, the amount of money paid by the manufacturer will be refunded by the provider. However, it's necessary to measure a physical property in order to see if the freight is compliant with the predefined rules or not. Therefore, the Blockchain has no power over that measurement -which can be carried out by a sensor or a human- and is incapable of assuring that the provided information is legit and not malicious.¹³⁵ There are many approaches which try to solve this issue on a technical way, but so far there is none which achieved success.¹³⁶

There are two possible options to fight against the described oracle problem:

- To introduce a TTP or remove the trust challenge among the parties: A TTP could be in charge of introducing the data to the Blockchain assuring that it's not malicious or, given a certain level of trust among the parties, the data introduced could be understood as legitimate. However, the requirements detailed for a Blockchain to be better suited over a centralized database are the impossibility

¹³⁴ John Adler and others, 2018, p. 1.

¹³⁵ Wüst and Gervais, 2017, fols 4–6.

¹³⁶ Adler and others, 2018, fols 1–2.

of finding an always online TTP and the lack of trust among the writers. Therefore, this approach would inherently discard Blockchain as a solution.

- Create a tamper-proof data collection system: If a technological development is able to provide with incorruptible sensors which are able to ensure the legitimacy of the collected data as well as proving themselves to be infallible and capable to introduce the gathered information into the Blockchain in a tamper-proof system, the benefits from a permissioned Blockchain should be applicable within the IoT in order to improve a given supply chain management.

Lastly, supply chains dedicated to digital products (i.e. music, movies, papers etc...) are not affected that heavily by the oracle problem. There are many initiatives within the cryptocurrency market which try to create a link between the artist and the consumer, removing the central party. However, those initiatives are not further discussed on this thesis since they rely on a cryptocurrency exchange.

4. Results

The initial systematic literature review which focused on explaining the mechanisms as well as the theoretical potential and applications for both Blockchain and the Internet of Things revealed many possibilities and value-adding opportunities derived from their technological adoption and implementation. It has been found as well, that given an interaction among Blockchain and IoT, the first one would work as a database-type enabling technology for the latter, which is a paradigm entailing different technologies both physically and digitally wise. However, two major flaws were encountered concerning the current literature which analyses the possible benefits of using Blockchain within the IoT:

- 1) There is no explanation about the real utility which the defined Blockchain use case within the IoT entails. Therefore, it's not clear who could get benefited from it or where and when could it be applied. As an example to better illustrate that, Blockchain could indeed provide a solution for IoT systems in order to create a decentralized environment, but maybe there is no requirement for that decentralization at all.
- 2) There is no proper comparison between Blockchain and other technologies which are able to provide the same utility. Maybe Blockchain is indeed able to contribute with a real use case, but another technology provides it as well in a faster, cheaper or more efficient way.

Furthermore, the review on possible models to study interaction among various technologies concluded that there is few well defined methodologies and only general frameworks were extracted. Those frameworks together with the above described major flaws on the literature have been put together in order to generate a systematic methodology to study the possible interactions as described on section 2.3.3 Specific model . Using this approach, it was possible to extract the following conclusions:

- Within the 6 major IoT adoption barriers identified, 15 elemental challenges which need to be faced in order to achieve wider adoption have been found (3.2.1 IoT elemental challenges).
- Within the 3 major Blockchain properties, 9 basic use cases have been found (3.2.2 Blockchain basic use cases)

- From this 15 elemental IoT challenges, it has been concluded that 4 of them could be solved or improved thanks to the Blockchain mechanisms (3.2.3 IoT Challenge Blockchain use cases match)

Given this information, the next steps on the methodology were meant to compare Blockchain with the currently used centralized databases and afterwards, if any successful match with outperforming potential was found, to carry out an analysis of their impact on the logistic sector. However, even if both Blockchain and centralized systems work as databases with the common aim of storing data it has been found that there is no use on comparing them on an overall level, since their inherent properties make them better suited for completely different scenarios. Three scenarios were found:

- 1) “There aren’t multiple writers” OR “It’s possible to use an always online TTP” OR “All witters are known and trusted”
- 2) “There are multiple writers” AND “It’s not possible to use an always online TTP” AND “Not all writers are known”
- 3) “There are multiple writers” AND “It’s not possible to use an always online TTP” AND “All writers are known” AND “Not all writers are trusted”

Since centralized databases offer better performance in terms of throughput and latency, they are the best option for the first scenario while for the second and third situations, Blockchain seems to be a better suited alternative. However, those scenarios are theoretical and it might be hard to find them on the real world. The analysis shows that the first one is the most likely to be found, the second one is the one regarding distributed or decentralized initiatives (C2C) such as Bitcoin or other cryptocurrencies and the third one is the one which might be applicable into logistics. The reasons found concerning the logistic sector which makes it a valid scenario for the integration of Blockchain in the IoT are the following:

- There is an obvious need to store data
- The supply chain is almost always formed by different parties with a need to interact.
- There are scenarios where there’s a desire of removing a TTP –either because it makes the process more complicated or because there’s no possibility of finding one-
- All the parties which might have writing powers are probably known but not that probably trusted.

From the use case perspective, it has been proved that the interaction between Blockchain and IoT has an application on the real world and that the logistics sector could benefit from it. However, a major inconvenient regarding the use of Blockchain in scenarios where there is a need of communication between the physical and digital world has been found and that's the case of IoT and moreover, logistics. This inconvenient, known as the oracle problem, can be defined as the incapability of proving the authenticity and legitimacy of the data which is introduced into the Blockchain. That means that even if Blockchains are capable of assuring the integrity of the data once it has been introduced in the chain, it provides with no mechanisms to check if the introduced data is legitimate or not in the first place. In order to overcome that issue, two possibilities are identified:

- To introduce a TTP or remove the trust challenge among the parties: A TTP could be in charge of introducing the data to the Blockchain assuring that it's not malicious or, given a certain level of trust among the parties, the data introduced could be understood as legitimate. However, the requirements detailed for a Blockchain to be better suited over a centralized database are the impossibility of finding an always online TTP and the lack of trust among the writers. Therefore, this approach would inherently discard Blockchain as a solution.
- Create a tamper-proof data collection system: If a technological development is able to provide with incorruptible sensors which are able to ensure the legitimacy of the collected data as well as proving themselves to be infallible and capable to introduce the gathered information into the Blockchain in a tamper-proof system, the benefits from a permissioned Blockchain should be applicable within the IoT in order to improve a given supply chain management.

Due to that oracle problem, models which rely entirely on the digital environment (e.g. music distribution, energy exchange among individual peers, data sharing, digital assets exchange etc...) are the only Blockchain use cases which are proven to be truly useful and to add benefits over the previous models. However, those models are built on top of a cryptocurrency background due to their C2C nature and offer little help towards the objectives which this thesis pursues. Summarizing the above findings, IoT and Blockchain interaction has a theoretical use case potential both on an overall and logistics-oriented scenario, but there are challenges which need to be overcome before that potential can be transferred to the real world.

5. Discussion

This section contains the author's view on the major flaws and limitations which the thesis entails and the future lines of research that should follow this work.

5.1 Criticism

The present project contains a systematic review on the current literature, defining the state of art for both Blockchain and IoT as well as a methodological approach to study if there's a possible interaction among them which could benefit the logistic sector in any way. However, both the systematic review and the methodological approach hold an incompleteness issue as a major flaw. This issue can be explained by four reasons:

- Blockchain as a whole: While speaking about the Blockchain on the previous chapters, only a distinction among permissioned/permissionless and open/private has been made. Furthermore, there was always the assumption of the network being well distributed and therefore, empirically tamperproof. However, there is multiple Blockchain consensus methods which define the security level as well as the energetic efficiency. Moreover, every consensus method (e.g. Proof of Work, Proof of Stake, Byzantine Agreement etc...) would probably have a best suited scenario and it should be analysed. Understanding the particularities of the logistic sector and Blockchain application on the supply chain management, it seems that Byzantine Agreements –or variations- should be the most attractive alternatives. They are the best suited when finding consensus among known, unique and fixed set of participants who determine consensus, but the coordination among peers could endanger the network.¹³⁷ In any case, further investigation among the different consensus methodologies and their value-adding capabilities as well as impediments within the defined interactions among Blockchain and Internet of Things should be carried out.
- Isolated approach: It has been stated that IoT should be understood as a paradigm with many enabling technologies. By being potentially Blockchain one of those, a study about how could IoT get benefited from it as well as an analysis on the value-adding scenarios have been carried out. However, by understanding that there are many technologies –both physical and digital- working together, it seems reasonable to state that they should be studied along with Blockchain. For

¹³⁷ Debus, 2017, p. 19.

instance, the development of RFID chips and sensors could play an enormous role on this interaction since items should be uniquely identified at any time and therefore, the price of those chips and sensors alone could be enough to determine the possibility or not of implementing a Blockchain-IoT derived system. In Figure 19 a first approach about possible future developments and research needs is included, but it's far from being sufficient. Furthermore, in the results sections it's possible to understand how the oracle problem makes almost impossible for Blockchain implementation on the supply chain to be a reasonable alternative. In order to solve that oracle problem, a technical solution is required. This technical solution could consist on a physical improvement on the sensors reliability and therefore the legitimacy of the introduced data or, on the other hand, it could refer to a consensus development which is able to solve the oracle problem without adding further inconveniences.

- Hype and selling purpose: As said, during the last years, and mostly during 2017, Blockchain technology as well as cryptocurrencies –such as Bitcoin or Ethereum- and other related companies became really famous, and it experienced a large growth, with a peak of over 800B\$¹³⁸. That ended being one of the biggest bull markets in the human history and therefore, many companies tried to benefit from it. On the one hand, technological consulting companies specialized on Blockchain made a biased divulgation campaign from which the mainstream media echoed. In the internet is possible to find many documents that speak about Blockchain use cases which have been proven as unreasonable in this thesis, not because Blockchain is not able to provide with a solution, but because there are easier and more efficient ways to do it or because it brings no value at all. On the other hand, companies decided to implement Blockchain just as a

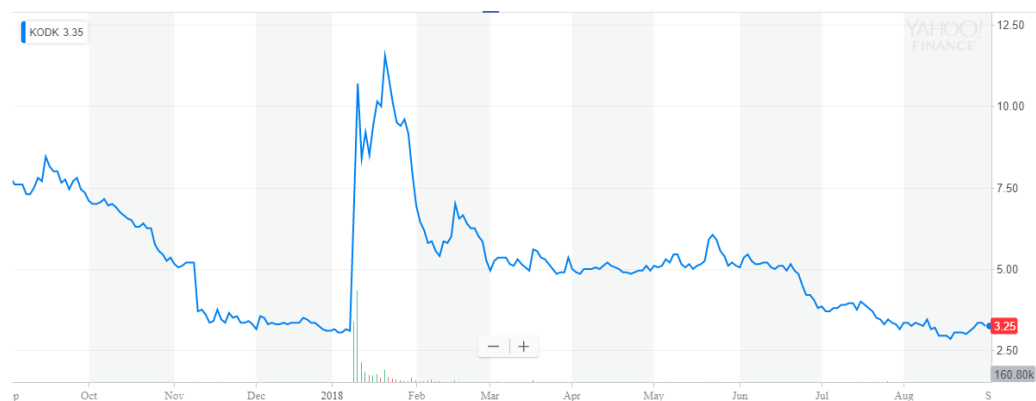


Figure 24: Kodak's stock price in USD. Sep'2017-Sep'2018. (Source: Yahoo Finance)

¹³⁸ 'CoinMarketCap', 2018.

promotion measure in order to improve their visibility on the mainstream media and gain new investors and followers. For example, Kodak announced the 9th of January of 2018 the launch of a Blockchain-backed system which sent the price from 3,15\$ to 10\$ in less than two weeks (Figure 24).¹³⁹ Nowadays the price is settled back to 3,25\$. Due all this expectations, a relatively large amount of the published literature is positive biased towards Blockchain and its future adoption. Therefore, even if the review was carried out through a critical and scientific perspective, there is an inherent risk of overestimation of the Blockchain capabilities and use cases.

- Insufficient comparison: When comparing Blockchain with other database centralized technologies as IoT enablers, it is possible to observe that they attend to different use cases and therefore they are better suited for different scenarios. However, on those scenarios where Blockchain might be better suited than centralized databases, it's still necessary to remark that there are other types of decentralized data storage systems which could provide with better solutions than Blockchain. Some examples in regard of technologies which Blockchain should be compared towards could be decentralized databases (e.g. Cassiopeia) as well as other append-only databases (e.g. Git).

Despite those flaws and limitations, the thesis brings a pragmatic and down-to-earth approach regarding actual Blockchain possibilities within the IoT and its current application scenarios on the logistic sector.

5.2 Future research

Considering the above mentioned limitations and in order to make this study more complete and accurate, the research topics which should be further analysed and reviewed are listed below.

- Technical comparison among Blockchain and other decentralized and append-only databases and systems.
- Further investigation in regard of the different consensus method's implications on the overall system efficiency and scenarios where they should be applied or discarded.

¹³⁹ Yahoo Finance, 2018.

- Investigate the IoT involved technologies, their possible development and how could they interfere or benefit Blockchain's adoption within the paradigm.
- Investigate the possible impact of Blockchain use within the IoT for the end user, observing if and how the derived improvements on the supply chain management could end up benefiting the final customer.

6. Final remarks

As of today, it is still unclear how the logistic sector could be benefited from the interaction between Blockchain and IoT. On a speculative and technical level, it is possible to observe that Blockchain properties are able to provide with solutions for the IoT paradigm in terms of data management, privacy and security. However, when studying the case in a thorough way and comparing Blockchain with centralized systems while clearly defining the possible given scenarios which emanate from the use of IoT within the supply chain management, it is possible to determine that the barrier located between the digital and the physical world –the oracle problem- works as a major challenge to be faced in order to embrace wider adoption.

Despite this lack of positive results in regard of Blockchain application on a logistic level, it has been found as well that in scenarios where this barrier between the digital and physical world does not play a big role it is possible to find some benefits from its use and new ways to carry out tasks. However, even the most ethereal of Blockchain applications, the exchange of digital assets (e.g. Bitcoin), needs to face this issue if it expects to be fully decentralized and benefit from smart contracts in order to go beyond the fact of just being a digital currency or to work as store of value. That means that even if a given Blockchain relies on a fully digitalized environment, it will be used by and for human beings which live on a physical world and the barrier will always exist. Its scale is the only thing which will vary. In order to illustrate that, if the Peer A lends some money to the Peer B through a Blockchain to help him finance a new business idea, with the condition of Peer B returning the amount in case of success, its necessary for someone to introduce into the Blockchain that the business was successful –or not- and in order to do that, again, it is necessary to trust someone. Hence, it doesn't matter if it is within the IoT or not, Blockchain needs to overcome the oracle problem in order to unleash its fully potential and it needs to do so even more if it aspires to be truly useful for the logistic sector.

As explained on the previous section, the thesis focuses on providing with a pragmatic approach and takes into consideration the needs and resources which we have nowadays. Therefore, even though the found results are mainly negative and discouraging, there are many variables which play a big role in the Blockchain and IoT synergy and this issue should be further analysed before completely discarding its benefits both on an overall and a logistic related area. Following this thread, the proposed

future research lines will undoubtedly help to gain a better understanding about this interaction and its upcoming perspectives as well as possible applications.

Bibliography

- Adler, John, Ryan Berryhill, Andreas Veneris, Zissis Poulos, Neil Veira, and Anastasia Kastania, 'Astraea: A Decentralized Blockchain Oracle', 2018 <<http://arxiv.org/abs/1808.00528>>
- Al-fuqaha, Ala, Senior Member, Mohsen Guizani, Mehdi Mohammadi, and Student Member, 'Internet of Things: A Survey on Enabling', 17 (2015), 2347–76 <<http://ieeexplore.ieee.org.proxy.queensu.ca/document/7123563/>>
- Alice, Bob, 'What Is a Blockchain?', *Deloitte*, 2016, 4–7 <<https://doi.org/10.1016/j.neuron.2016.11.015>>
- 'Apple Inc. (AAPL)' <<https://finance.yahoo.com/quote/AAPL/?guccounter=1>> [accessed 15 May 2018]
- Ashton, Kevin, 'That "Internet of Things" Thing - RFID Journal.Pdf', *RFID Journal*, 2009 <<https://doi.org/10.1145/2967977>>
- BitFury Group, and Jeff Garzik, 'Public versus Private Blockchains. Part 1: Permissioned Blockchains', *Bitfury*, 2015, 1–23 <<http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf>>
- Boritz, Efrim, 'Views on Core Concepts of Information Integrity', *University of Waterloo Centre for Information Systems Assurance*, 2003, 27
- Brajović, Vladimir, 'When Are Smart Sensors Smart? An Example of an Illumination-adaptive Image Sensor', *Emerald Group Publishing Limited*, 2013
- Charu C, Aggarwal, 'Managing and Mining Sensor Data', 2013, 1–545 <<https://doi.org/10.1007/978-1-4614-6309-2>>
- 'CoinMarketCap', 2018 <www.coinmarketcap.com> [accessed 15 May 2018]
- Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin, 'Blockchain for the Internet of Things: A Systematic Literature Review', 2016 *IEEE/ACS 13th*

International Conference of Computer Systems and Applications (AICCSA), 2016, 1–6 <<https://doi.org/10.1109/AICCSA.2016.7945805>>

Crosby, Michael, and Pattanayak Pradan, 'BlockChain Technology: Beyond Bitcoin', *Applied Innovation Review*, 2016

Debus, Julian, 'Consensus Methods in Blockchain Systems', 2017, 1–58

DHL, and Accenture, 'Blockchain in Logistics - Perspectives on the Upcoming Impact of Blockchain Technology and Use Cases for the Logistics Industry', 2018, 28 <<https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf>>

Dutsch, Gunther, and Neon Steinecke, 'Use Cases for Blockchain Technology in Energy & Commodity Trading', *PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft*, 2017, 20 <www.pwc.com>

FDA, 'Data Integrity and Compliance With CGMP (Draft)', *FDA Guidance for Industry*, 2016, 20993–2 <<http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>>

Finance, Yahoo, 'Eastman Kodak Company (KODK)', 2018 <<https://finance.yahoo.com/quote/KODK/chart?p=KODK&.tsrc=fin-srch>> [accessed 2 September 2018]

Gigli, M, and Koo S., "Internet of Things: Services and Applications Categorization," *Advances in Internet of Things*, *Scientific Research*, 1 No. 2 (2011), 27–31 <<https://doi.org/10.4236/ait.2011.12004>>

Harvard Business Review, 'Internet of Things: Science Fiction or Business Fact?', *Harvard Business Review*, Analytics (2014), 8>

House, David, Gordon E Moore, and International Technology Roadmap, 'Moore ' s Law', 2015

Hsu, Chin-Lung, and Judy Chuan-Chuan Lin, 'An Empirical Examination of Consumer Adoption of Internet of Things Services: Network Externalities and Concern for

- Information Privacy Perspectives', *Computers in Human Behavior*, 2016
<<https://doi.org/10.1016/j.chb.2016.04.023>>
- Iansiti, Marco, Karim R Lakhani, and Hassan Mohamed, 'The Truth about Blockchain', *Harvard Business Review*, 2017
<https://enterpriseproject.com/sites/default/files/the_truth_about_blockchain.pdf>
- IBM, 'Banking Use Cases', 2018 <<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=92014192USEN>> [accessed 20 May 2018]
- IBM, 'Financial Markets Use Cases', 2018 <<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=91014191USEN>> [accessed 21 May 2018]
- IDC, 'Internet of Things Spending Guide', 2014
- Kersten, Wolfgang, Thorsten Blecker, Christian M Ringle, Niels Hackius, and Moritz Petersen, 'Blockchain in Logistics and Supply Chain: Trick or Treat?', *Digitalization in Supply Chain Management and Logistics*, 9783745043 2017, 18
<<https://doi.org/10.15480/882.1444>>
- Koomey, Jonathan G., Stephen Berard, Marla Sanchez, and Henry Wong, 'Implications of Historical Trends in the Electrical Efficiency of Computing', *IEEE Annals of the History of Computing*, 2011 <<https://doi.org/10.1109/MAHC.2010.28>>
- Kowallick, Stefanie, 'How Blockchain Can Help to Prevent Odometer Fraud', 2017
<<https://blog.bosch-si.com/blockchain/how-blockchain-can-help-to-prevent-odometer-fraud/>> [accessed 20 May 2018]
- Krawiec, RJ, Dan Barr, Jason Killmeyer, Mariya Filipova, Florian Quarre, Allen Nesbitt, and others, 'Blockchain: Opportunities for Health Care', *NIST Workshop on Blockchain & Healthcare*, 2016, 1–12
<<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf>>
- Lee, In, and Kyoochun Lee, 'The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises', *Business Horizons*, 58 (2015), 431–40

<<https://doi.org/10.1016/j.bushor.2015.03.008>>

Luthra, Sunil, Dixit Garg, Sachin Kumar Mangla, and Yash Paul Singh Berwal, 'Analyzing Challenges to Internet of Things (IoT) Adoption and Diffusion: An Indian Context', in *Procedia Computer Science*, 2018 <<https://doi.org/10.1016/j.procs.2017.12.094>>

Macaulay, James, Lauren Buckalew, and Gina Chung, 'Internet of Things in Logistics', *DHL Trend Research*, 1 (2015), 1–27

Mahajan, Saurabh, 'Blockchain a Technical Primer', *Deloitte Insights*, 2018 <<https://www2.deloitte.com/insights/us/en/topics/emerging-technologies/blockchain-technical-primer.html>>

Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and others, 'The Internet of Things: Mapping the Value beyond the Hype', *McKinsey Global Institute*, 2015, 144 <https://doi.org/10.1007/978-3-319-05029-4_7>

'Md5hashgenerator' <www.Md5hashgenerator.com> [accessed 16 May 2018]

Nakamoto, Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System', *Www.Bitcoin.Org*, 2008, 9 <<https://doi.org/10.1007/s10838-008-9062-0>>

Nordrum, Amy, 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated', *IEEE Spectrum*, 2016

O'Halloran, Derek, and Elena Kvochko, 'Industrial Internet of Things : Unleashing the Potential of Connected Products and Services', *World Economic Forum*, 2015, 40 <<https://doi.org/10.1111/hcre.12119>>

Ouaddah, Aafaf, Anas Abou Elkalam, and Abdellah Ait Ouahman, 'FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things', *Security and Communication Networks*, 9 (2016), 5943–64 <<https://doi.org/10.1002/sec.1748>>

Patel, Keyur K, and Sunil M Patel, 'Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges',

International Journal of Engineering Science and Computing, 6 (2016), 6122–31
<<https://doi.org/10.4010/2016.1482>>

PowerLedger, 'How Does the Technology Work?' <<https://tge.powerledger.io/faq.php>>
[accessed 23 May 2018]

Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Chi Yang, 'The Blockchain as a Decentralized Security Framework [Future Directions]', *IEEE Consumer Electronics Magazine*, 7 (2018), 18–21
<<https://doi.org/10.1109/MCE.2017.2776459>>

Rahman, Mahmudur, Hua-Jun Hong, Amatur Rahman, Pei-Hsuan Tsai, Afia Afrin, Md Yusuf Sarwar Uddin, and others, 'Adaptive Sensing Using Internet-of-Things with Constrained Communications', *Proceedings of the 16th Workshop on Adaptive and Reflective Middleware*, 2017, 6:1--6:6 <<https://doi.org/10.1145/3152881.3152887>>

Renault, 'Groupe Renault Teams with Microsoft and VISEO to Create the First-Ever Digital Car Maintenance Book Prototype', 2017
<<https://media.group.renault.com/global/en-gb/media/pressreleases/94238/groupe-renault-microsoft-et-viseo-sassocient-pour-cree-le-premier-prototype-de-carnet-dentretien-nu1>> [accessed 24 May 2018]

Rimba, Paul, Xiwei Xu, Ingo Weber, and An Binh Tran, 'Comparing Blockchain and Cloud Services for Business Process Execution', *IEEE International Conference on Software*, 2017

SBI Group, 'SBI Ripple Asia', 31/03/2018, 2018
<<https://www.sbigroup.co.jp/english/company/group/sbirippleasia.php>> [accessed 16 May 2018]

Shaik, Khwaja, 'Why Blockchain and IoT Are Best Friends', *IBM*, 2018

Shrestha, Ajay Kumar, and Julita Vassileva, 'Towards Decentralized Data Storage in General Cloud Platform for Meta-Products', *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies - BDAW '16*, 2016, 1–7 <<https://doi.org/10.1145/3010089.3016029>>

- Smith, Andy, and Cecilia Cran, 'Santander Becomes First UK Bank to Introduce Blockchain Technology for International Payments with the Launch of a New App', 27/05/2015, 2015 <https://www.santander.com/csgs/Satellite?applD=santander.wc.CFWCSancomQP01&canal=CSCORP&cid=1278712674240&empr=CFWCSancomQP01&leng=pt_PT&pagename=CFWCSancomQP01%2FGSNoticia%2FCFQP01_GSNoticiaDetalleImpresion_PT48>
- Steffen, Søren, and Lars Ramkilde, 'Cryptographic Hash Functions', 2009
- Tapscott, Don, and Alex Tapscott, 'Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies', *Whitepaper*, 2017, 46 <www.weforum.org>
- Utterback, James M, Robert M Mason, Louis A Lefebvre, and M Tarek, 'A Lotka-Volterra Model for Multi-Mode Technological Interaction: Modeling Competition, Symbiosis and Predator Prey Modes', 1996, 62–71
- VeChain, 'Use Cases' <<https://www.vechain.org/enterprise/#usecases>> [accessed 20 May 2018]
- Vermesan, Ovidiu, and Peter Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, *Scientific American*, 2004, CCXC1 <<https://doi.org/10.1038/scientificamerican1004-76>>
- Wüst, Karl, and Arthur Gervais, 'Do You Need a Blockchain?', *IACR Cryptology EPrint Archive*, 2017, 1–7
- Yousuf, Tasneem, Rwan Mahmoud, Fadi Aloul, and Imran Zualkernan, 'Internet of Things (IoT) Security : Current Status , Challenges and Countermeasures', 5 (2015), 608–16 <<https://doi.org/10.20533/ijisr.2042.4639.2015.0070>>
- Zhang, Zhi Kai, Michael Cheng Yi Cho, Chia Wei Wang, Chia Wei Hsu, Chong Kuan Chen, and Shiuhyng Shieh, 'IoT Security: Ongoing Challenges and Research Opportunities', *Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014*, 2014, 230–34 <<https://doi.org/10.1109/SOCA.2014.58>>

