



**Universidade do Minho**  
Escola de Engenharia

Rui Pedro Roriz Mendes de Sousa Fernandes

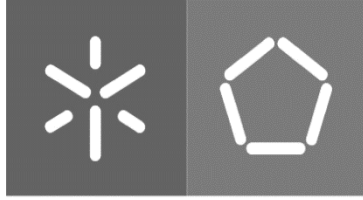
## **Blockchains & Smart Contracts: Exploratory Analysis**

Dissertação de Mestrado Integrado em Engenharia e Gestão  
de Sistemas de Informação

Trabalho efetuado sob a orientação de  
Professor Doutor José Luís Mota Pereira

Outubro de 2018





**Universidade do Minho**  
Escola de Engenharia

Rui Pedro Roriz Mendes de Sousa Fernandes

## **Blockchains & Smart Contracts: Exploratory Analysis**

Dissertação de Mestrado Integrado em Engenharia e Gestão  
de Sistemas de Informação

Trabalho efetuado sob a orientação de  
Professor Doutor José Luís Mota Pereira

Outubro de 2018

## DECLARAÇÃO

**Nome:** Rui Pedro Roriz Mendes de Sousa Fernandes

**Endereço Eletrónico:** a64865@alunos.uminho.pt

**Telefone:** 911918112

**Número do Cartão de Cidadão:** 14321479

**Título Dissertação:** Blockchain and Smart Contracts: Exploratory Analysis

**Orientador:**

Professor Doutor José Luís Mota Pereira

**Ano de conclusão:** 2018

Mestrado Integrado em Engenharia e Gestão de Sistemas de Informação

É AUTORIZADA A REPRODUÇÃO INTEGRAL DESTA TESE/TRABALHO APENAS PARA EFEITOS DE INVESTIGAÇÃO, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE;

Universidade do Minho, \_\_\_/\_\_\_/\_\_\_

Assinatura: \_\_\_\_\_

***“An engineer knows he has achieved perfection  
not when there is nothing left to add, but when  
there is nothing left to take away”***

Adapted from Antoine de Saint-Exupéry



## **Acknowledgments**

The realization of a master's degree dissertation is without a doubt, a long journey with a lot of dedication, challenges, joys, sorrows, doubts and uncertainties, but this path is only possible to make with the support and incentive, direct or indirect, of some people to whom I am eternally grateful.

To my advisor, Professor José Luís Mota Pereira for the trust placed in me for the realization of this topic, the total support and availability on its concretization, opinions and critics which made the investigation evolve, total collaboration on resolving problems and doubts which came along the way and for all the words of encouragement.

To my parents, Luzia Roriz and Armando Fernandes, a sincere vote of gratitude, for the education instilled in me along these years that made me the person I am today.

To my brother, Armando Jorge for the good mood he has that always encouraged me in the more tough times.

To Margarida Beir, which lived close this moment of hard work and never let me give up, believing always on my capabilities. Also, for all the help given for the development of this dissertation.

In general, gratitude to all my family and friends that contributed in some way for the completion of this work.





## **Abstract**

Blockchain is a relatively new technology created for Bitcoin's network to store transaction records happening in it. The system is redundant and distributed, making it difficult for corrupt transactions. Without doubt the greatest use case of this technology is cryptocurrencies, however is wrong to restrict this tool only to the financial area. Many use cases are also being developed for business areas like digital identity and technological areas like IoT and many other areas.

Due to the complexity, privacy and bureaucracy of certain processes in many areas a new technology rise called Smart Contracts, computational code programmable to meet certain conditions. These digital contracts act like traditional contracts, with the difference of its automaticity, where the need for a notary and certified people to validate signatures can be erased.

So, the point of this thesis is to understand the concept of Blockchain and Smart Contracts and how they can be integrated together in other business and technological areas to improve and increase the efficiency of the organizational processes. After that, to create a demonstration case that show all the potential behind these technologies in a business area.



# i. Index

<b>Acknowledgments</b> .....	i
<b>Abstract</b> .....	iii
<b>1. Introduction</b> .....	1
1.1 Contextualization .....	1
1.2 Objectives .....	2
1.3 Methodology Approach .....	3
1.4 Document Structure .....	5
<b>2. Concepts and Fundamentals in Blockchain</b> .....	9
2.1 Introduction .....	9
2.2 Concepts .....	10
2.2.1 Blockchain .....	10
2.2.2 Distributed Ledger .....	12
2.2.4 Smart Contracts .....	13
2.2.5 Consensus Mechanism .....	16
2.2.6 Blockchain Types .....	17
2.3 How a Blockchain works .....	19
2.3.1 Definition of codes (Hash) .....	19
2.3.2 Creation of the Blocks .....	20
2.3.3 Chain of Blocks .....	23
2.3.4 Chains of Chains (Blockchain) .....	24
2.4 Blockchains Technologies .....	27
2.4.1 Ethereum .....	27
2.4.2 Hyperledger Fabric .....	27
2.4.3 Multichain .....	28
2.5 Conclusion .....	29

<b>3. Areas for Blockchain application</b> .....	31
3.1 Introduction .....	31
3.2 Business areas for Blockchain .....	32
3.2.1 Finance Industry .....	32
3.2.2 Digital Identity Industry.....	34
3.2.3 Property Title Industry .....	35
3.2.4 Communication Industry .....	36
3.3 Technologic areas for Blockchain .....	37
3.3.1 IoT.....	37
3.3.2 BigData .....	40
3.3.3 BPM .....	41
3.3.4 AI .....	45
3.4 Conclusion .....	47
<b>4. The Insurance Domain</b> .....	49
4.1 Introduction .....	49
4.2 Insurance History .....	50
4.3 Car Insurance.....	51
4.4 Frauds.....	52
4.5 Conclusion .....	55
<b>5. Blockchain Demonstration Case</b> .....	57
5.1 Introduction .....	57
5.2 Architecture and Business Process.....	58
5.3 Tools .....	62
5.4 Demonstration.....	66
5.5 Conclusion .....	85
<b>6. Conclusion</b> .....	87

**References** ..... 93

**Annex A – Cientific Publication: IoT applications using Blockchain and Smart Contracts**  
..... 101



## ii. Figure Index

Figure 1 - Design Science Research Methodology Process Model .....	4
Figure 2 - How a Blockchain works.....	11
Figure 3 - Smart Contract example .....	14
Figure 4 - Smart Contract life cycle.....	15
Figure 5 - Blockchain Types .....	18
Figure 6 - Empty SHA256 Hash example.....	20
Figure 7 - "Blockchain" Hash .....	20
Figure 8 - Valid Block .....	21
Figure 9 - Invalid Block.....	22
Figure 10 - Valid Block after mining.....	22
Figure 11 - Distributed ledger valid example .....	23
Figure 12 - Invalid Distributed Ledger .....	24
Figure 13 - Example of valid Blockchain .....	25
Figure 14 - Invalid Blockchain with corrupted node .....	26
Figure 15 - Survey on Blockchain Thought Leaders.....	32
Figure 16 - BPM Six Core Elements.....	42
Figure 17 - Client Server architecture .....	58
Figure 18 - Solution based on Blockchain.....	59
Figure 19 - Car insurance creation process "AS IS" .....	60
Figure 20 - Car insurance creation with Blockchain "TO BE" .....	60
Figure 21 - Blockchain solution architecture for Insurance Companies .....	61
Figure 22 - Solidity logo .....	62
Figure 23 - node.js logo .....	62
Figure 24 - Truffle framework logo.....	63
Figure 25 - Ganache logo .....	64
Figure 26 - MetaMask logo.....	65
Figure 27 - Sublime logo .....	65
Figure 28 - Ganache interface .....	66
Figure 29 - Smart Contract used in the system .....	67
Figure 30 - MetaMask interface .....	69

Figure 31 - MetaMask connecting to the right network .....	69
Figure 32 - MetaMask choosing the right network .....	69
Figure 33 - Private key of an account .....	70
Figure 34 - MetaMask exporting private key for creating account.....	71
Figure 35 - MetaMask choosing right account.....	71
Figure 36 - Blockchain solution interface .....	72
Figure 37 - Insurance creation form .....	72
Figure 38 - Insurance creation example.....	73
Figure 39 - MetaMask user transaction confirmation after form submitted.....	74
Figure 40 - Ganache transaction confirmation of success.....	75
Figure 41 - All the insurances linked to an account of an insurance company.....	75
Figure 42 - Error caught by the Smart Contract for not being valid .....	76
Figure 43 - Error message for failed transaction .....	77
Figure 44 - Claim creation form.....	77
Figure 45 - Claim transaction user confirmation .....	78
Figure 46 - Transaction confirmation after being submitted.....	79
Figure 47 - All claims linked to the wallet of an insurance company .....	79
Figure 48 - End Insurance interface.....	80
Figure 49 - Select shows all active insurances .....	80
Figure 50 - All data related to the insurance selected appears.....	81
Figure 51 - Confirmation of the transaction end insurance .....	82
Figure 52 - Confirmation of the insurance submitted into the Blockchain.....	83
Figure 53 - After ending an insurance it gets an end date .....	83
Figure 54 - Car history records.....	84



### **iii. Table Index**

Table 1 - Research work objectives.....	2
Table 2 - Methodology phases versus dissertation chapters .....	5
Table 3 - Matrix chapters versus objectives.....	6
Table 4 - Blockchain technologies comparison .....	28



## **iv. Acronyms**

*AI – Artificial Intelligence*

*API – Application Programming Interface*

*BPM – Business Process Management*

*DApp – Decentralized Application*

*DDoS - Distributed Denial-of-Service*

*DL – Distributed Ledger*

*DLT – Distributed Ledger Technology*

*DPoS – Delegated Proof of Stake*

*CSS – Cascading Style Sheets*

*EVM – Ethereum Virtual Machine*

*FTP – File Transfer Protocol*

*HTTP – Hypertext Transfer Protocol*

*ICT – Information and Communication Technologies*

*IDE – Integrated Development Environment*

*IoT – Internet of Things*

*PBFT – Practical Byzantine Fault Tolerance*

*PoW – Proof of Work*

*PoS – Proof of Stake*

*PoA – Proof of Authority*

*SHA – Secure Hash Algorithms*



# 1. Introduction

## 1.1 Contextualization

The financial world moves a lot of money every day and many people make use of it. However, the system is full of problems, additional costs like fees and delays, bureaucracy and opportunities for criminal activities like fraud and crime. For instance, 45% of financial intermediaries (PricewaterhouseCoopers, 2014), like services for money transfer and stock exchanges experienced some sort of crime every year. For the entire economy the number is about 37%. So, this is an important concern for banks because regulatory costs continue to increase (Medland, 2015). All these problems have costs to the institutions consequently the consumer must pay for it (Tapscott & Tapscott, 2017).

Considering all these problems, on 2008, Satoshi Nakamoto, author of bitcoin, published and described the way to a peer-to-peer payment system, based in electronic coin, Bitcoin (Nakamoto, 2008). Months later, the source code was published to allow any person to participate in a network of payments (Nakamoto, 2009). Over the years, Bitcoin has risen in terms of popularity, although the technology which makes Bitcoin work remains unknown, but it came to stay and to revolutionize many business areas.

The technology is called Blockchain and consists in a set of nodes interconnected, with the same set of records replicated by all. These records are divided into blocks which consist in transactions between the nodes. When a transaction is made the information corresponding to it is broadcasted to all the nodes, so they can add it to their distributed ledger.

A second generation of Blockchain technologies introduced the Smart Contract's concept. Smart Contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code and executed automatically when an event or a condition is met. Introduced in 1995 by Nick Szabo (Szabo, 1997), his concept definition isn't too far from what Smart Contracts are being built for. A simple example, a cable-TV supplier and a client established a contract with a set of clauses which basically, estipulate the conditions in which the service is supplied by the first and paid by the second. Using the Smart Contract concept, when a clause is disrespected by anyone (the service was off during a period, date of payment was exceeded, etc.) a set of pre-defined actions are automatically executed (reduction of the amount to pay by the client proportional to service down-time or when the client exceeded the limit time to pay).

The potential of both technologies alone is high and combining the two could bring more secure and reliable systems. So, the challenge is to understand the different areas of business and how could these two technologies help to improve them.

## 1.2 Objectives

Blockchain is clearly, a technology with high growth within the global market. However, and before making changes, organizations need to understand how this technology may help them improving their performance, whether on a business level or on a technological level.

Therefore, understanding and exploring this technology created the main objective of this dissertation, “Blockchain and Smart Contracts: Exploratory Analysis”. Furthermore, since the author already had personal experience in developing Blockchain Solutions, it was decided that another objective should be applying the acquired concepts to the development of a Blockchain demo.

To fulfill the main objective of this thesis, a set of four objectives was defined. These objectives are gathered in Table 1 and will be described in a more detailed way in the subsequent paragraphs.

*Table 1 – Research work objectives*

<b>OBJECTIVE IDENTIFIER</b>	<b>OBJECTIVE DESCRIPTION</b>
<b>01</b>	Review fundamentals and literature of Blockchain and Smart Contracts
<b>02</b>	Study of economical areas with potential for Blockchain solutions
<b>03</b>	Being fluent with a programming language related to Blockchain and Smart Contracts
<b>04</b>	Development of a Blockchain Solution with support for Smart Contracts

First Objective (O1 – Review fundamentals and literature of Blockchain and Smart Contracts) – This objective consists in the review and analysis of scientific articles related with the Blockchain and Smart Contracts concepts. The point was to make a solid knowledge base capable of supporting all the research work in order to understand and describe, in a detailed level, how both technologies work, what it needs to function, etc.

Second Objective (O2 – Study of economical areas with potential for Blockchain solutions) – After understanding the concepts of Blockchain and Smart Contracts and how they work, the point is to search for business areas where their potential could help. As explained in the previous section, Blockchain has already made a major impact in the financial market so the challenge is to make the same impact in others business areas and which processes are modified by this technology.

Third Objective (O3 - Being fluent with a programming language related to Blockchain and Smart Contracts) – When the theme of this dissertation was suggested by the Professor José Luis Mota Pereira, one of the end results he was expecting to be accomplished was the development of a solution that could demonstrate all the potential of the technologies. So, this objective is important because to develop a solution of this kind is necessary to have knowledge about a programming language related to the technologies, otherwise the solution cannot be developed.

Fourth Objective (O4 – Development of a Blockchain Solution with support for Smart Contracts) - This last objective combines all the previous objectives and work done to make a Blockchain Solution. So, after understanding the concept, research enough information and study all the business areas with viability to integrate Blockchain, an area is chosen, and a Blockchain Solution is developed for that area integrating some of its processes.

### **1.3 Methodology Approach**

Given the complexity and importance of a master thesis, is necessary to adopt an approach which helps in the execution of the research work. For this end, a reflection was made regarding how the study should be conducted so all the objectives could be met in a stipulated time.

This reflection began by analyzing which is the role and the importance of research methodologies. With that, a general view of many investigational methodologies was obtained and a personal knowledge about the importance of them. After the analyses made and having always the nature of the problem in mind, it was selected the one regarded as more adequate.

With the result from this reflection, it was decided a set of three sequential activities based in Design Science Research (DSR), which formalized the strategy adopted to fulfill the goals of this work. This methodology is divided into 5 phases (Peffer, Tuunanen, Rothenberger, & Chatterjee, 2007):

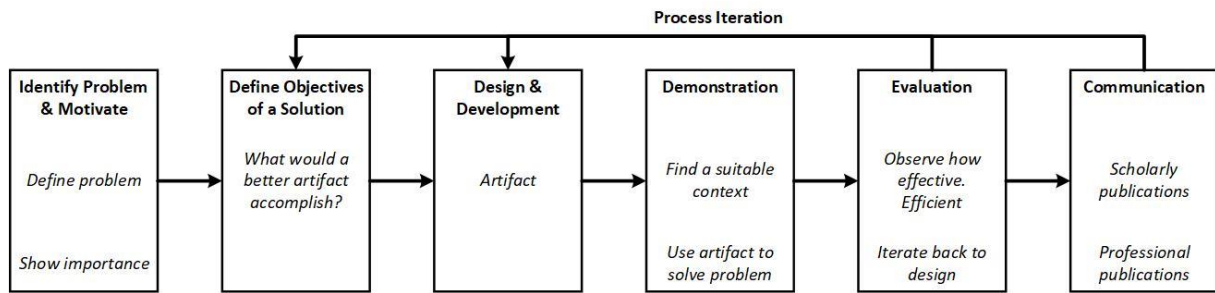


Figure 1 - Design Science Research Methodology Process Model (Peppers, Tuunanen, Rothenberger, & Chatterjee, 2007)

First phase is Identify Problem & Motivation where a description of the problem found is made as well as the importance to solve it. Here, the main goal, is to answer a set of generic questions, for instance, what is the problem to solve, what should be done to solve this problem and what are the goals. The output of this phase is a proposal for a new research effort and other benefits like understand what is going to be achieve and a strategy for the entire research.

The second phase is Define Objectives of a Solution. This phase relates to the first because here is where we're going to establish the objectives to achieve. The output of this phase is a set of objectives which are going to guide us through the entire project. As we accomplished them, we walk towards our final solution.

Third phase is Design & Development and here is where the artifact is made. Conceptually, an artifact can be any object conceived in which there is some research contribution to its development. The output of this phase is a Blockchain solution enriched with Smart Contracts which can demonstrate all the potential of the technologies involved.

Fourth phase is Demonstration. After the implementation of the artifact here we demonstrate it. With this phase, it is expected that one or more instances of the problem are answered by the artifact. The demonstration can involve the utilization of the artifact in experiences, simulations, use cases and others.

The fifth phase is Evaluation. Here is where we observe if the solution developed is efficient and effective enough to give a solution for the problem. The utility, the quality and the effectiveness of an artefact must be demonstrated by using relevant metrics and analysis techniques. Depending on the nature of the problem, the evaluation can assume multiple forms, for instance, studying the artefact in controlled environment to evaluate their qualities like usability or comparing the functionalities of the artefact with the objectives to the solution referred in the second activity.

In the end of this phase, the output is results on how our solution perform against the problem and if the results are not good enough, the investigator can decide to go back to the third activity (Design &



Development) to improve the effectiveness of the artefact or go back to the second activity (Define Objectives of a Solution) to redefine the objectives.

The last phase is Communication. This is where we communicate everything related to the project. We show to researchers and other relevant people our problem and its importance and the utility, the innovation and the efficiency of our artefact to answer it.

Table 2 - Methodology phases versus dissertation chapters

<b>Phases</b> <b>Chapters</b>	<b>Identify Problem &amp; Motivate</b>	<b>Define Objectives of a Solution</b>	<b>Design &amp; Development</b>	<b>Demonstration</b>	<b>Evaluation</b>	<b>Communication</b>
<b>1.</b> Introduction	X	X				
<b>2.</b> Concepts and Fundamentals in Blockchain			X			
<b>3.</b> Areas for Blockchain application			X			
<b>4.</b> Application of Insurance Domain				X	X	
<b>5.</b> Blockchain Demonstration Case				X	X	
<b>6.</b> Conclusion						X

### 1.4 Document Structure

This document consists in all the research work done for the thesis until this moment and is a way of exposing the theme in study. Next, it is described the organization of this document summarizing the 4 chapters constituting it.

The chapter 1, begins with a contextualization of the thesis’s theme and how relevant is in today’s world. After that, the objectives that are set to achieve are described, as well as the methodologic approach adopted. At last, the organization of the document is described, where it is shown how it is organized and what subjects are covered throughout.

The chapter 2 is structured in 3 sections, where, over the sections, it is explained everything related to Blockchain and Smart Contracts. In the first section, it is shown all the important concepts involving the technology which help defining the area of study of this thesis. The second section has a more in-depth explanation on how Blockchain works. The last section, features Blockchains applications for different areas.

The chapter 3 is organized only in two sections, presenting areas with high potential for a Blockchain integration. On the first section, cases more oriented for business areas are discussed and, on the second section, cases that are more oriented for other innovative technologies.

The chapter 4 has all the information related to Insurance because since the developed system has the objective of ending with a problem about Insurance, is important to understand how it works. The chapter starts with a brief history about the subject and how it evolved during the years. Then, everything related to car insurance, in Portugal, is explained to understand how it works. In the last section, examples of the most common fraud insurances and the fraud that is going to be used for the developed system are shown.

The last chapter (5), refers to the system developed using Blockchain. It is divided into 3 sections: "Architecture and Business Process", "Tools" and "Demonstration". In the first section an "AS IS" without Blockchain and a "TO BE" with Blockchain is shown. It has also an architecture of the system to developed. The second section describes all the tools used in the development. The third section has the description of all the new processes using Blockchain.

Table 3 - Matrix chapters versus objectives

	<b>01</b>	<b>02</b>	<b>03</b>	<b>04</b>
<i>Chapter 1</i>				
<i>Chapter 2</i>	X			
<i>Chapter 3</i>		X		
<i>Chapter 4</i>		X		
<i>Chapter 5</i>			X	X

The table 2 relates each one of the dissertation chapters with the objectives established for the research work. The first objective is Review fundamentals and literature of Blockchain and Smart Contracts and it is covered throughout the dissertation, however it has more focus in the second chapter because is only reserved for learning all the concepts related to Blockchain and Smart Contracts.

The point of the second objective (Study of economical areas with potential for Blockchain solutions) is to see how the current applications and system have incorporated Blockchain into their processes. The chapter 3 "Areas for Blockchain application" is exclusive for this objective, business and technological areas are analyzed to see the most relevant applications.

The third and the fourth objectives (Being fluent with a programming language related to Blockchain and Development of a Blockchain Solution with support for Smart Contracts) are very connected to each

other. By developing a Blockchain solution inevitably improve skills of the corresponding language which is being used, so by accomplished one objective the other comes along. For fulfilling these two objectives, the chapter 5 is where everything related to the development of the solution is discussed.



## **2. Concepts and Fundamentals in Blockchain**

### **2.1 Introduction**

*"If I have seen further than others, it is by standing upon the shoulders of giants" – Isaac Newton*

Concepts and Fundamentals are very important in any scientific work, since it makes a reference to what has already been discovered about the researched subject, thus avoiding loss of time on unnecessary quests. In addition, it helps on the work which is going to be made. Is a tough activity because every text written on this document needs a previous reflection of the information gathered so the texts produced can have good arguments and conclusions. Is a section of the document which contains insights from multiple authors and articles published in magazines, conferences, journals and books.

In this chapter, the concepts and fundamentals of Blockchain were made in three sections. Initially, on the first (1) section, the concept of Blockchain is introduced and explained. Since Blockchain is a very complex technology, it is also important to understand other concepts that are inevitably related to it, like, Smart Contracts, Distributed Ledger and Consensus Mechanism.

Afterwards, in the second (2) section, a more detailed explanation on how Blockchain works in practice is presented. It is explained how cryptographic hashes are used and how they are combined to maintain the logic of the chain.

In the last section (3), it is shown the most relevant Blockchain's technologies from which one is going to be picked to be used in this dissertation.

## 2.2 Concepts

### 2.2.1 Blockchain

On the 31st of October of 2008, an article was published by someone under the name of Satoshi Nakamoto, called “Bitcoin: A Peer-To-Peer Electronic Cash System”. In this article, some of the features of Bitcoin, who have the potential to revolutionize the financial sector, were shown:

- Enable direct transactions without the need for trusted third parties;
- Enable non-reversible transactions;
- Reduce credit cost in small casual transactions;
- Reduce transaction fees;
- Prevent double-spending.

With these features, Satoshi Nakamoto, intended to create *“an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.”* (Nakamoto, 2008).

Through this initial idea, the bases for the creation of Bitcoin were established and later (9<sup>th</sup> of January of 2009) the first Bitcoin application was created. However, the success of the bitcoin comes from a cryptographic technology underlying it, namely the Blockchain technology (Pilkington, 2015). Many have separated Blockchain technology from the Bitcoin application, so they can use it in other industries (Nofer, Gomber, Hinz, & Schiereck, 2017). *“This is much more than the financial services industry. Innovators are programming this new digital ledger to record anything of value to humankind – birth and death certificates, marriage licenses, deeds and titles of ownership, rights to intellectual property, educational degrees, financial accounts, medical history, insurance claims, citizenship and voting privileges, location of portable assets, provenance of food and diamonds, job recommendations and performance ratings, charitable donations tied to specific outcomes, employment contracts, managerial decision rights and anything else that we can express in code.”* (Tapscott & Tapscott, 2016). Because of all this potential, 10 years after the creation of Bitcoin, it is estimated that more than 25 countries are investing in Blockchain technology, making more than 2500 patents and making a total of 1.3 billion dollars invested (McWaters, 2016).

**But, how do we define this technology?**

“A Blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties.” (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2015).

All the transactions or digital events are inserted into blocks and these are added to the Blockchain in a linear, chronological order (Swan, 2015).

To be added in a chronological order, the blocks need to be validated before being added. A validation is made by a consensus protocol mechanism. In bitcoin the mechanism is called proof-of-work (PoW). To make this mechanism work, there is a group of people in the network called “miners”. Their job consists in changing one variable until the network accepts the solution (Seffinga, Lyons, & Bachmann, 2017). The solution is met, the validation was made and the miner who found the solution transmits the new block to all the nodes participating in the network, so they can add it to their distributed ledger. For the effort of mining, the miner is rewarded in bitcoins (See Figure 2).

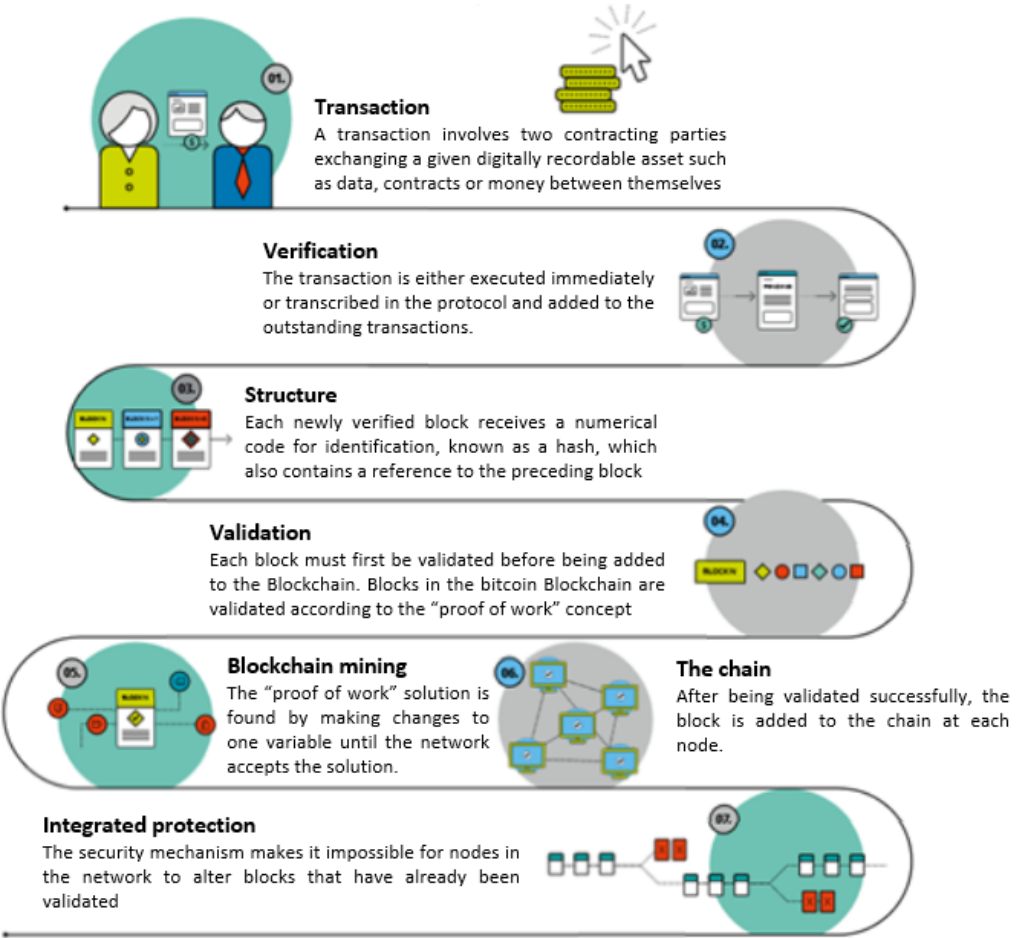


Figure 2 - How a Blockchain works (Seffinga, Lyons, & Bachmann, 2017)

With this process, Blockchain brings a new paradigm to the online business. Its strengths include (Savelyev, 2017):

- **Transparency:** all the data on Blockchain is public, it cannot be arbitrarily tempered, and it is easily auditable.
- **Redundancy:** every node of the Blockchain solution holds a copy of the data, thus it cannot be easily taken offline due to a system malfunction or malicious actions of third parties.
- **Immutability:** changing records in a Blockchain is prohibitively difficult and requires consensus provided in accordance with the protocol (e.g., by the majority of Blockchain users). Thus, integrity of records is ensured by intrinsic properties of the underlying code rather than from the identities of system operators.
- **Disintermediation:** the removal of middlemen, such as banks or collective societies, from transactions decreases transaction costs and risks associated with presence of such intermediaries. It does not mean, however, that a new kind of intermediaries will not be created as a result of deeper implementation of Blockchain technologies in the social fabric.

### **2.2.2 Distributed Ledger**

A distributed ledger is an asset database that can be shared across a network on multiple sites, geographies, or institutions. All users within the system can have access to the ledger via copy or connection to the larger database. Any changes made on any one of the ledgers will be reflected on all the ledgers that currently exist (Walport, M. G. C. S. A., 2016).

In 117 AC, the roman empire reached the largest size in all his history (Mark, 2011). However, despite distances a banking system was a reality in that time and it was designed for an individual to deposit sums of money in any location within the empire. Due to the existence of currency that allowed for the purchase of trading in investment, finance, and real estate, the romans used a kind of distributed ledger which used paper checks (Negro & Tao, 2013). With the high number of complex business transactions occurring in the empire, records keepers kept their distributed ledger in a very precise way and transferring information between banks to maintain the records accurate with technological precision (Smith, 1875).

Distributed Ledger Technology (DLT) allow their users to reach consensus on a version of the distributed ledger, on the sequential order of transactions. This means that there cannot be any doubt as to the users' respective holdings. Central validation is replaced in a DLT by a set of cryptographic solutions



and economic incentives that combine to prevent illicit updates and reconcile discrepancies. The ledger produced can thus be considered authoritative, although its management is shared among users with conflicting incentives (Pinna & Ruttenberg, 2016).

In traditional centralized database architectures, everything relies on a single entity to store data. This entity is controlled by a central administrator whose job is to maintain the integrity of the stored data. Generally, there is a security system which protects the raw data from external attacks (Benos, Garratt, & Gurrola-Perez, 2017).

Distributed databases are an alternative version of databases. Instead of a central storage, the database (or copies of it) is spread across the network and is stored at different physical locations. The control is usually centralized, and the integrity is also provided by a central administrator and a centralized application is used to manage the database and synchronize. The nodes are trusted, and access is controlled by the network administrator (Benos, Garratt, & Gurrola-Perez, 2017).

A distributed ledger (DL) is a distributed database because every node has a synchronized copy of the database, however there are three characteristics that differentiate it from the traditional concept (Benos, Garratt, & Gurrola-Perez, 2017):

1. Decentralization: The central authority (administrator) is eliminated and the integrity is achieved using a consensus mechanism or validation protocol. The control of the database (read/write access) is decentralized, this means every node of the network participates in it. There is no need for a central administrator to ensure the integrity of the data or its consistency across nodes. Instead, this is achieved through some consensus mechanism or validation protocol.
2. To ensure integrity of the database, a consensus mechanism is used, this is way we can implement DL in a trust-less environment where the parties involved may not fully trust each other.
3. Cryptographic encryption: The ledger uses cryptographic encryption tools to deliver (1) and (2) above.

#### **2.2.4 Smart Contracts**

In 1997, Nick Szabo published an article called "The idea of Smart Contracts". He defined Smart Contract as *"A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are 'smarter' than their paper-based ancestors"* (Szabo, 1997).

Despite the definition being two decades old, it stills adheres well to today's reality. If we dissect the definition and analyze the keywords, it will be present in other's definitions in our days. Nick Szabo said, *"we could make a set of promises"* and according to Christidi and Devetsikiotis *"We trigger a Smart Contract by addressing a transaction to it. It then executes independently and automatically in a prescribed manner on every node in the network, according to the data that was included in the triggering transaction."* (Christidi & Devetsikiotis, 2016) . We can program a Smart Contract to behave like we want, and the output will be like we promised (Figure 3).

*"Smart Contracts have been designed to automate transactions and allow parties to agree with the outcome of an event without the need for a central authority."* (Cant, et al., 2016). Nick described Smart Contracts as *"protocols within which the parties perform"*, so when a transaction or an event occurs there is a set of rules who tells how the data should be processed helping to produce the right outcome.

As *"in other forms of digital electronics"* we accomplish this by transforming the Smart Contract into lines of codes with clauses and agreements embedded as code within the software. Smart Contracts seek to leverage the trustless, immutable nature of the Blockchain to empower peer-to-peer, disintermediated agreements enforced automatically by code (Brennan & Lunn, 2016).

```

/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then communicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw; // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw; // Check allowance
    balanceOf[_from] -= _value; // Subtract from the sender
    balanceOf[_to] += _value; // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw; // Prevents accidental sending of ether
}

```

Figure 3 - Smart Contract example (Rosic, 2017)

## Life cycle of decentralized Smart Contracts

The life cycle of a Smart Contract typically consists of four broad phases: Create, Freeze, Execute and Finalize (See Figure 4).

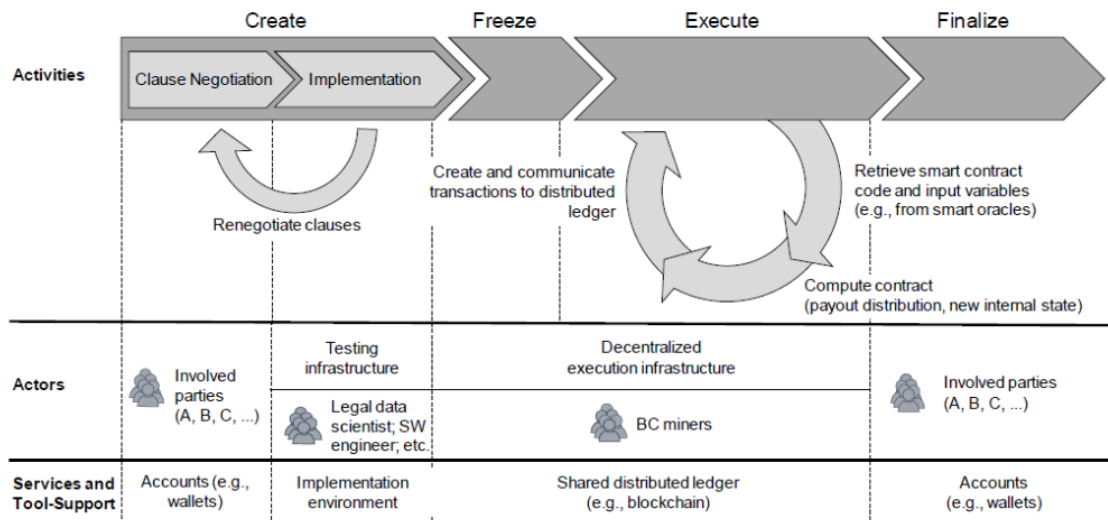


Figure 4 - Smart Contract life cycle (Sillaber & Waltl, 2017)

**Create:** First, the parties involved need to agree on the objectives of the contract, similarly to a classic contract negotiation. After everything is settled, the contract needs to be turned into code. Most Smart Contract environments have a proper infrastructure to create, maintain and test the contract and with that we can validate the behavior and content of the contract. This process of converting requirements into code may take several iterations between the negotiation and implementation so the stakeholders and programmers agreed in what is done. After the parties agree, the contract is then submitted to the distributed ledger (Sillaber & Waltl, 2017).

**Freeze:** After the Smart Contract has been submitted to the Blockchain, it is persisted by a majority confirmation of the participating nodes. In exchange for this service, and to prevent a flooding of the ecosystem with Smart Contracts, a fee has to be paid to the miners. From this point onward, the contract and all parties are public and accessible through the public ledger.

During the freeze phase, any transfers made to the wallet address of the Smart Contract are frozen and the nodes take on the role of a governance board, ensuring the preconditions for executing the contract are met.

**Execute:** All the participant nodes can read the contracts stored in the distributed ledger. The code is executed by the inference engine of the Smart Contract environment after the contract's integrity is

validated. The execution of the Smart Contract results in a set of new transactions that passed through all the conditions of the contract.

**Finalize:** After the Smart Contract has been executed, the new state of information is validated through the consensus protocol and broadcasted to all the nodes. The prior committed digital assets are transferred (unfreezing of assets) and with the confirmation of all transactions, the contract has been fulfilled.

### **2.2.5 Consensus Mechanism**

Literally, consensus mean is agreement. Consensus algorithms are those algorithms that help a distributed or decentralized network to unanimously take a decision whenever necessary. Its features include assuring decentralized governance, quorum structure, authentication, integrity, non- repudiation, byzantine fault tolerance and performance (Sankar, Sindhu, & Sethumadhavan, 2017).

There are multiple Consensus Mechanisms in the Blockchain universe and they are the validation mechanism, the rules to a network automatically validate a transaction. Consensus is required to maintain the world state of the Blockchain network. Key to the operation of the Blockchain is that the network should collectively agree on the contents of the ledger: instead of authority for keeping accounts being centralized in one entity, like a bank, it is shared amongst everyone.

#### **Examples of Consensus Mechanisms**

**Proof-of-Work (PoW)**, as explained before, consists on solving complex mathematical equations before they can validate transactions and insert blocks into the Blockchain. This process is called mining, and miners are responsible for it. Solving these mathematical problems is very hard, however is easy to verify. After these problems are solved, miners are rewarded by their work with the corresponding digital currency, known as block reward. If the miners are mining on the Bitcoin Blockchain, they're rewarded in Bitcoin (Liu & Camp, 2006).

**Proof-of-Stake (PoS)** aims to replace the way of achieving consensus in a distributed system; instead of solving the Proof-of-Work (PoW), the node which generates a block must provide a proof that it has access to a certain amount of coins before being accepted by the network. Generating a block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called target) is specified by the network through a difficulty adjustment process like PoW that ensures an approximate, constant block time. The selection based on account balance is quite unfair because the single richest

person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block (Vasin, 2014).

**Delegated Proof of Stake (DPoS)** – Developed by Daniel Larimer, it was envisioned to fight the high consumption of energy of Bitcoin mining and he predicted that Bitcoin mining would become centralized in the future because of the giant mining pools controlling the entire network. He also agreed the way PoW is designed is too slow and there should be another way, faster, of validating transactions. He decided to name it Delegated Proof-of-Stake or DPoS (Larimer D. , 2014). DPoS and traditional PoS are very different. One makes use of a democracy based on elected or chosen representatives the other uses a direct democracy. In regular PoS, every wallet that contains coins is able “stake”, in other words, they can participate in the process of validating transactions and forming the distributed consensus and earn coins in return. In a DPoS system, every wallet that contains coins is a stakeholder and can elect their delegates to generate and validate blocks. Using this system helps reducing the validation time of a block because of the number of nodes to validate it. An application that uses this system is Bitshares (Larimer D. , 2017).

**Proof-of-Authority (PoA)** – Using the idea of identity as stake, PoA tries to decrease the time that transactions take on private chains. Unlike PoW, it does not need miners resolving mathematical problems to validate a transaction, instead uses validators, authorized accounts that have the power of creating new blocks and secure the Blockchain. Individuals of the network can earn the right of becoming a validator, so there is an incentive to retain the position and every validator needs to perform well to increase his reputation. To become a validator is not easy, it can be necessary to obtain a public notary license to ensure the validator is credible, as well, as his identity must be formally verified (Arasev, 2018).

### **2.2.6 Blockchain Types**

As is known, Bitcoin’s system is available to everybody and anyone can participate in it. To the context where is inserted, it makes sense functioning in that way because the more people joins more nodes will be added increasing the size of the network and increasing its security. However, if we want to bring Blockchain to other contexts we must think if it is appropriate to apply the same concept of openness. Some organizations have crucial and private information that may not want to share it with other participants within the network and in Bitcoin’s paradigm everything related with transactions is shared. So, in this section, the point is to give some insight about all types of Blockchain (See Figure 5).

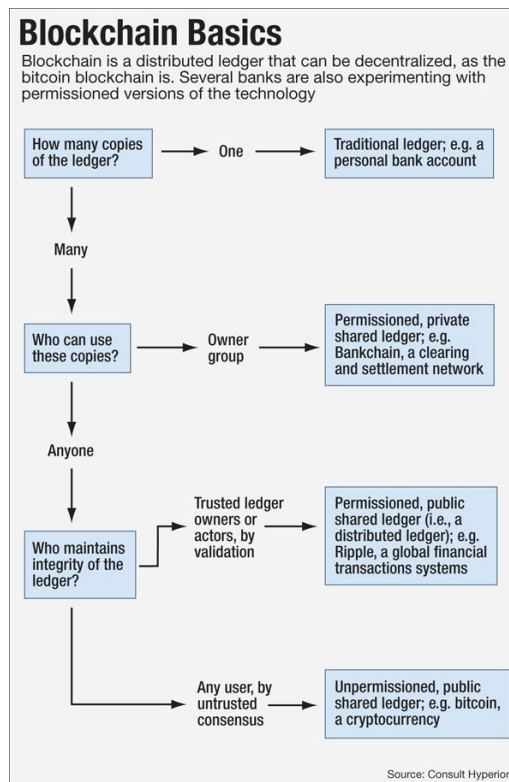


Figure 5 - Blockchain Types (Jentzsch, 2017)

### 2.2.6.1 Public Blockchains

Anyone can participate in a public Blockchain because it is open-source and public to all where no one is in charge. There is no access or rights management done for a public Blockchain and anyone can be part of the consensus.

The catch is that this type of self-governed, decentralized yet trustless autonomy is ensured on the system by its method of decision making which is very difficult or nearly impossible to tamper with. This decision making is called in this realm (Khatwani, 2017).

### 2.2.6.2 Private Blockchains

*“Private Blockchains provide interesting opportunities for businesses to leverage [their] trustless and transparent foundation for internal and business-to-business use cases. With the advent of Smart Contracts, this technology could eventually replace many centralized businesses.”* (O’Connell, 2016)

### 2.2.6.3 Consortium Blockchains

Consortium Blockchain is a Blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 3 entities for instance, Bank A, Bank B and a regulator node, each of which operates a node and of which, 3 must sign every block for the block to

be valid. The right to read the Blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the Blockchain state. These Blockchains may be considered “partially decentralized” (Whyte, 2017).

#### **2.2.6.4 Sidechains**

*“A sidechain is a Blockchain that validates data from other Blockchains”* (Back, et al., 2014). Can connect multiple Blockchains like financials and permission less into a single interconnected environment. The point of sidechains is to allow the transfer of assets from different Blockchains with an exchange rate. To implement such Blockchains, the protocols of both Blockchains must be aware of other chains (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2015).

### **2.3 How a Blockchain works**

To fully understand Blockchain, we need to understand its working mechanisms. So, this chapter is reserved to explain it. To support this explanation, we’re going to use a very interesting demo created by Anders Brownworth<sup>1</sup>.

#### **2.3.1 Definition of codes (Hash)**

When a transaction is made, it is grouped in a block cryptographically protected with other transactions that have occurred over the last 10 minutes and is broadcasted to all the network. Miners (network members with high levels of computational power) compete to validate transactions by solving complex mathematical problems. The first miner to solve a problem and validate the block is rewarded with a prize (in case of bitcoin the miner earns bitcoins as a payment).

To understand better Blockchain, it’s necessary to understand the method used to cryptograph blocks. SHA256, has a set of cryptographic hash functions which are applied in digital data to generate “digital fingerprint” of that data. In Figure 6, it is shown an example of how this SHA function works. It is noticeable the constitution of SHA algorithm, one text box (“Data”) which is empty (without data) and another box with “Hash” which in this case has the code:

“e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855” this set of numbers and letters corresponds to the empty hash.

---

<sup>1</sup> available in <https://github.com/anders94/Blockchain-demo>

## SHA256 Hash



The screenshot shows a web-based interface for calculating a SHA256 hash. It features a large, empty text input field labeled "Data:" and a smaller text output field labeled "Hash:" containing the hexadecimal string: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855.

*Figure 6 - Empty SHA256 Hash example*

To test the variable hash is necessary insert some data or information in the field “Data”. To give an example, the word “Blockchain” will be insert as is possible to verify in the Figure 7. After insert the word, automatically, the hash modifies passing the following code:

(625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1), in other words, according with the word inserted it was produced a new hash. It doesn't matter the quantity of data inserted, it can be many or few, the produced hash will always be the same to the same data.

## SHA256 Hash



The screenshot shows the same web-based interface as Figure 6, but now the "Data:" field contains the word "Blockchain". The "Hash:" field has updated to show the new hexadecimal hash: 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1. The hash field is highlighted with a red border.

*Figure 7 - "Blockchain" Hash*

Hash function is very simple to explain, however, as we add more variables and more blocks, the process starts to become more complex.

### **2.3.2 Creation of the Blocks**

After explaining how sha256 algorithm works, it is important in the next step understand how this mechanism works in a block.

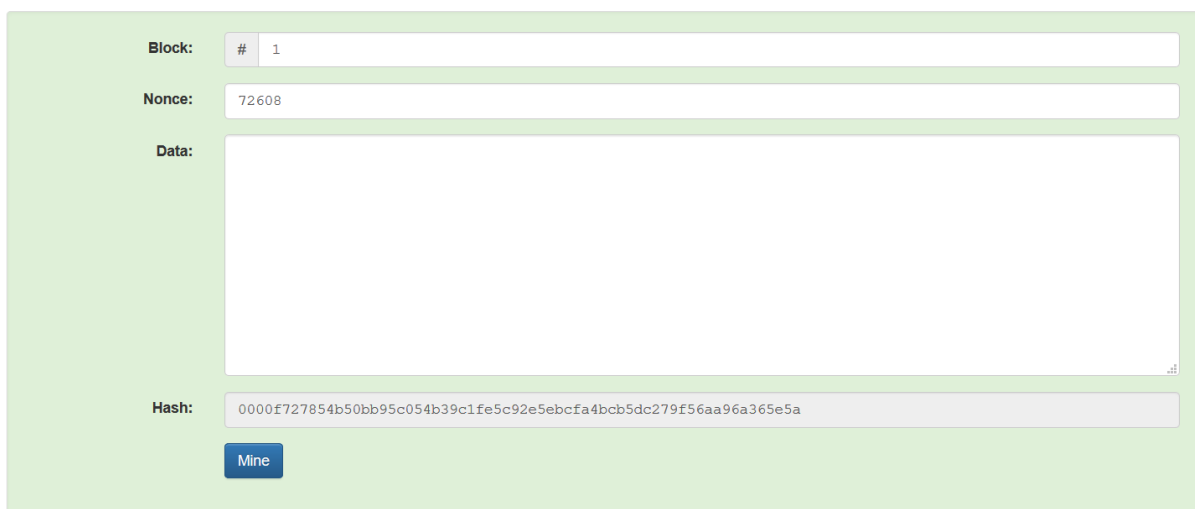
The method remains the same, the only difference is the addition of more fields as we can see in the Figure 8. The field “Block” appears, which corresponds to the number of the block who's going to be



created. The “Nonce” field is a numeric value assigned according with information written in “Data” field. This “Nonce” can be adjusted to try to find a number which make the hash value start with zeros.

In the Figure 8, we can verify that the hash’s value starts with 4 zeros. That means we are facing a peculiar hash, given most of the hashes don’t have this particularity, we conclude the block is valid. To this example, it is supposed that for a block to be considered valid, the hash needs to have four initials zeros. This can be predefined, we can have a Blockchain in which the block, to be valid, need to have more zeros. The advantage of having this characteristic is how much more zeros the hash has the more secure the network is, however, the process is slower.

## Block



The screenshot shows a web interface for block mining. It features four input fields: "Block:" with a dropdown menu set to "# 1", "Nonce:" with the value "72608", "Data:" which is an empty text area, and "Hash:" which displays the hexadecimal string "0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a". Below the hash field is a blue "Mine" button. The entire interface is set against a light green background.

*Figure 8 - Valid Block*

### **What happens if we changed something in the fields above the hash?**

Adding a new word like “Olá” to the field “Data”, the hash changed, losing the initial four zeros and the block acquires the red color. This happens because of our modification, we tried to corrupt the validated Block and because of that he shows that it is no longer valid. To make it valid again, it is necessary to assign numbers to “Nonce” until the hash starts with zeros again. That can be viewed in the Figure 9.

## Block



Block: # 1

Nonce: 72608

Data: Olá


Hash: 74db9336f742a8cb8476d64055a0bbae7599fa9e29c20a6b9e2663b593631d89

Mine

*Figure 9 - Invalid Block*

However, if the process is performed manually, in other words, if we insert random numbers, until we finally get the correct nonce it would take a long time. So, to solve this in an easier and quick way, it would be using the resources of computer – “Mine” – which means mining the block using the hash function and sha256 algorithm again to encrypt the block. This process is called mining.

## Block



Block: # 1

Nonce: 70286

Data: Olá

Hash: 00005094c7ed86ba6a26cd34afd52b76ed34ca50f7addb046aeb228befb384a0

Mine

*Figure 10 - Valid Block after mining*

Once we use the computational help which realizes automatically the mining – select button “Mine” – the block becomes valid. It is possible to verify that the hash starts with 4 zeros and the “Nonce”, which allows the block to become valid, is 70286, as is shown in the Figure 10.



## Blockchain

The image displays three sequential blockchain blocks, each with a 'Mine' button. The first block (Block # 1) is green and has a 'Data' field that is empty. The second block (Block # 3) is pink and has 'Blockchain!' in its 'Data' field. The third block (Block # 4) is also pink and has an empty 'Data' field. Each block's 'Prev' field contains the 'Hash' of the previous block, and its 'Hash' field is a SHA256 hash of its 'Data' and 'Prev' fields.

Block #	Nonce	Data	Prev Hash	Hash
1	11316		00	000015783b764259d382017d91a36d206d060e2cbb356f
3	12937	Blockchain!	000012fa9b916eb9078f8d98a7864e697ae83ed54f5146f	92df0c9ef23809394ce07e3f270d7cb9f084b21b4e1b66f
4	35990		92df0c9ef23809394ce07e3f270d7cb9f084b21b4e1b66f	d4a95d011b85b0adb6d1740be86390fa083c14e0e787e0f

Figure 12 - Invalid Distributed Ledger

At this moment, once how Blockchain works is explained, one needs to understand how it becomes distributed. In other words, how a distributed Blockchain is. Encryption mechanism is the same, SHA256 algorithm and the introduction of the block in the chain is made with the Prev field which shows the hash value of the previous block of that one.

### 2.3.4 Chains of Chains (Blockchain)

After describing the functioning of the chain of blocks, it is important to visualize how the all thing is organized. In the example below (Figure 13) 3 nodes are represented with their respective ledger (Peer A, Peer B, Peer C). They have the same copy of the Blockchain.

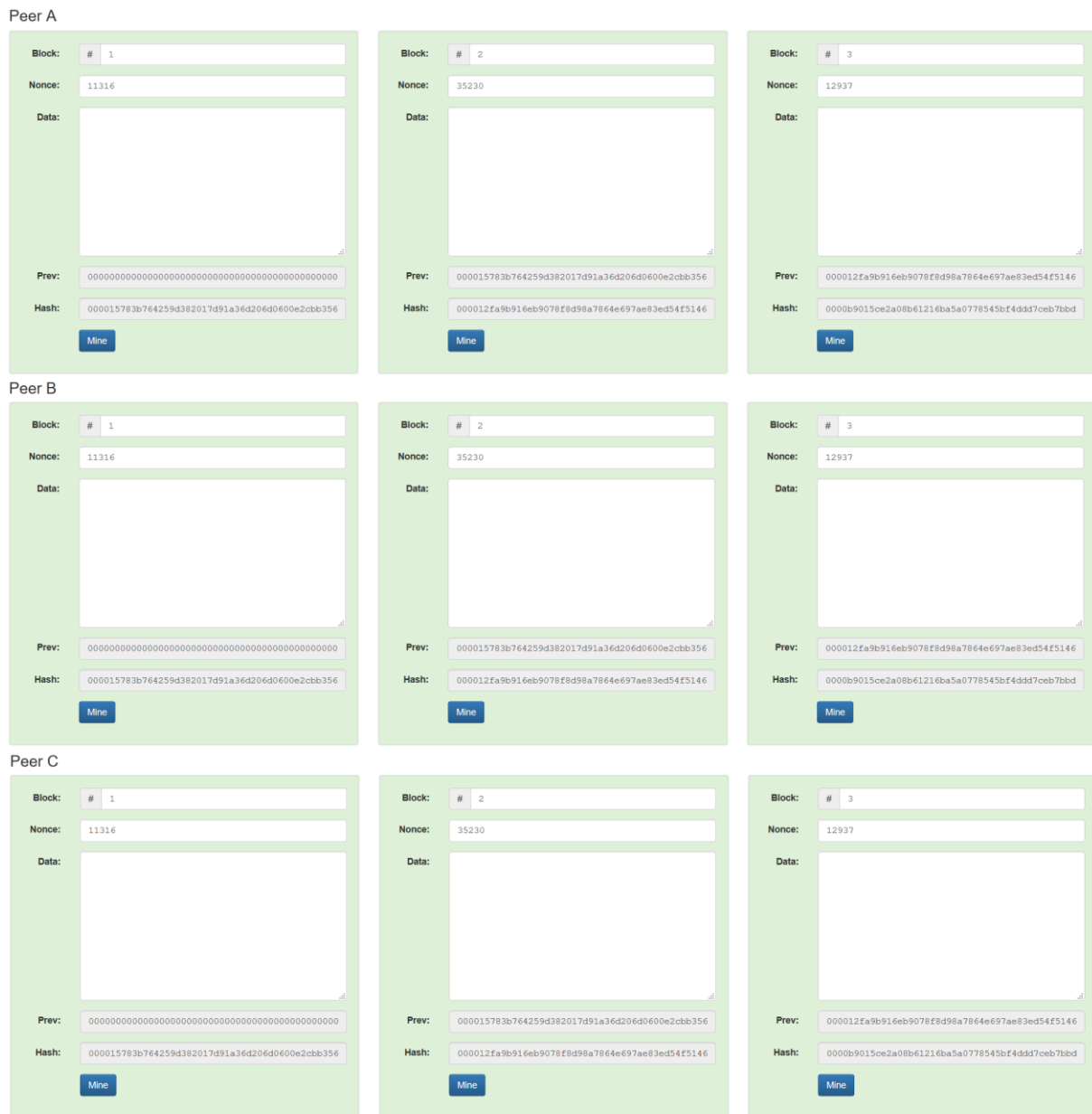


Figure 13 - Example of valid Blockchain

If we apply the same example given before and modify the second block of the Peer A (Figure 14), all the chain after that block turns invalid (red). Remaining those blocks would imply to get new hashes.

Comparing block 5 of peer A to block 5 of peer B and peer C, we see different hashes. Only peer B and peer C remain the same. Because of the two peers (B and C) having 5 equal blocks, it is deduced that something is wrong with peer A, even if all the hashes of peer A started with 4 zeros.

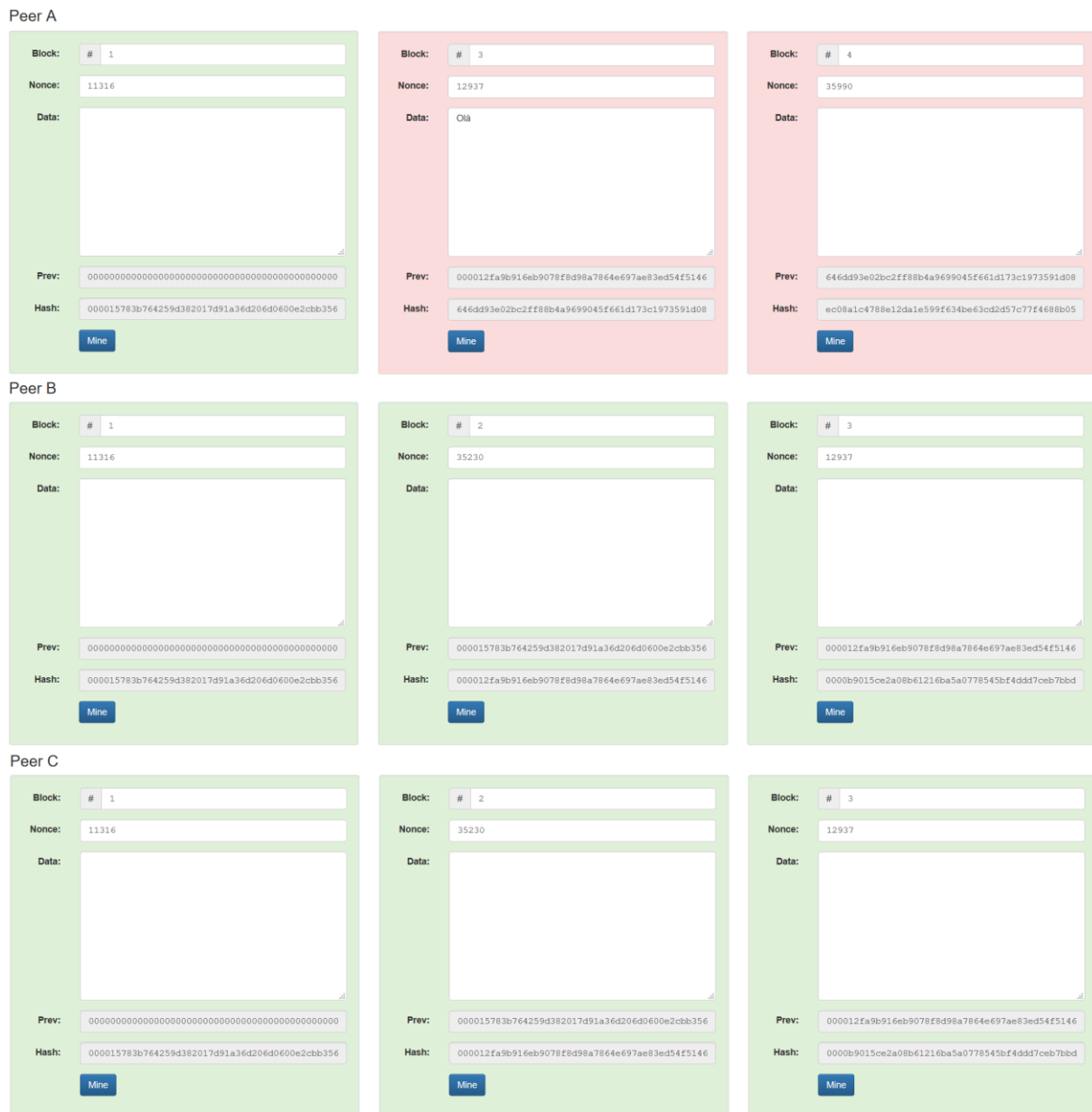


Figure 14 - Invalid Blockchain with corrupted node

That's how a Blockchain completely distributed works, having multiple copies in different nodes, everybody can easily verify if all the blocks are identical. A Blockchain can have a lot of blocks, so, instead of checking all of them one by one, we can only look to the hash of the most recent block (in this case in number 3) and see if something has been changed.

The block of valid transactions is then time stamped and added to the chain in linear and chronological way. New blocks of valid transactions are linked to older blocks, making the chain of blocks of all the transactions made in the history of that Blockchain. The entire chain is constantly updated so all the ledgers in the network are the same, giving to each member the ability to prove what one has at a given time.

## **2.4 Blockchains Technologies**

### **2.4.1 Ethereum**

Ethereum is a distributed platform that, besides the implementation of pre-defined function, is able to store and execute Smart Contracts and digital signatures, all from a Blockchain. The platform is supported by the Ethereum Virtual Machine (EVM). The value of the network is undeniably linked to the support of Smart Contracts. It is an open-source project which uses multiple programming languages, like Java and Python.

Ethereum can be considered as a public Blockchain, so its mode of operation is permission less as everybody can participate in the network. To maintain a consistent state of the ledger the order of the transactions is important. Besides that, every participant needs to reach consensus over the order of all transactions even if they haven't taken place in it.

The consensus mechanism of Ethereum is Proof of Work (PoW) but, because of PoW's high consumption of energy, eventually this mechanism will lead to a centralization, mainly because better machines are always needed, Ethereum is planning on changing to Proof of Stake (PoS) (Valenta & Sandner, 2017).

### **2.4.2 Hyperledger Fabric**

Hyperledger Fabric is an implementation of Blockchain technology with modular architecture which allows to connect multiple functions. It includes containers to host any mainstream language for Smart Contracts development. The mode of operation is permissioned, the access to the network is restricted to some participants previously chosen. This type of mode of participation, has a profound impact on how consensus is made.

Not every node in the network has the same role, they can be identified as clients, peers or orderers. A client is an end-user and creates transactions which are communicated to peers and orderers. He must connect to a peer for communicating with the Blockchain. Peers are responsible to maintain the ledger and add the messages of the orderers to commit new transactions to the ledger. Within the peers, there is a special one called Endorser whose task is to endorse a transaction by checking if they have the enough conditions. Every chain code can define these conditions for them to follow. Orderers or Ordering-service-node provide communication channels for peers and clients, so the messages, containing

transactions, can be broadcasted. Depending on the consensus, the channels make sure that every peer in the network gets the same messages with the same logical order (Hyperledger Fabric, 2017).

### 2.4.3 Multichain

Multichain is a product launched in 24<sup>th</sup> of July of 2015 by Coin Sciences, a company focused in the development of technologies and services for private Blockchains either within or between organizations. The product offers an “off-the-shelf platform” to create and implement private Blockchains which can be configured by the administrators of the systems, without the need of software programmers.

It uses a distributed consensus between identified block validators. Basically, is a PBFT (Practical Byzantine Fault Tolerance), but instead of multiple validators per block, there is one validator per block, working in a round-robin type of fashion.

Permissions in MultiChain is based in public key cryptography. Each user has a private key which is generated randomly, that they can never reveal to other participants. This private key has a mathematically related public address representing an identity for receiving funds. When sent to a public address, only using the private key can allow the funds to be spent and to “sign” a new transaction. Accessing to a private key, corresponds to ownership of any funds which it protects (Greenspan, 2015).

In the Table 4, is made a quick comparison between all the three technologies characteristics.

Table 4 - Blockchain technologies comparison

<i>Technologies</i>	<i>Description of platform</i>	<i>Governance</i>	<i>Data Structure</i>	<i>Mode of operation</i>	<i>Consensus mechanism</i>	<i>Smart Contracts</i>
<i>Ethereum</i>	Generic Blockchain Platform	Ethereum Foundation	Block	Permissionless, public or private	PoW (may change to PoS in the near future)	Smart Contract code (Solidity)
<i>Hyperledger</i>	Modular Blockchain Platform	Linux Foundation	Block	Permissioned, private	Multiple	Smart Contract code (Java)
<i>Multichain</i>	Off-theshelf platform	Coin Sciences	Block	Permissioned, private	PBFT (Practical Byzantine Fault Tolerance)	Smart Contract code (Java)



## 2.5 Conclusion

*“An investment in knowledge pays the best interest” – Benjamin Franklin*

As a brief conclusion of this chapter, it is important to emphasize three concepts, which are essential to the realization of the proposed objectives. Thus, the importance of this chapter is to define Blockchain, Smart Contracts and Distributed Ledger.

*“A Blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties.”* (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2015). All the transactions or digital events are inserted into blocks and these are added to the Blockchain in a linear, chronological order (Swan, 2015). To be added in a chronological order, the blocks needed to be validated before being added. A validation is made by a consensus protocol mechanism, in bitcoin the mechanism is called proof-of-work (PoW). To make this mechanism work, there is a group of people in the network called “miners”. Their job consists in changing one variable until the network accepts the solution (Seffinga, Lyons, & Bachmann, 2017). The solution is met, the validation was made and the miner who found the solution transmits the new block to all the nodes participating in the network, so they can add it to their distributed ledger. For the effort of mining, the miner is rewarded in bitcoins.

Distributed Ledger is a technological system that is an asset database that can be shared across a network on multiple sites, geographies, or institutions. All within the system can have access to the ledger via copy or connection to the larger database. Any changes made on any one of the ledgers will be reflected on all the ledgers that currently exist. Every node has a synchronized copy of the database.

Smart Contracts is *“A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are ‘smarter’ than their paper-based ancestors”* (Szabo, 1997).

In the next chapter it is shown how these concepts combine into solutions with potential to improve business and technological areas.



## **3. Areas for Blockchain application**

### **3.1 Introduction**

*“Stay away from it. It’s a mirage, basically” - Warren Buffet*

Currently, there is a very high expectation related to the future of Blockchain technology. Many startups are being created just to focus in the technology, while the big Information and Communication Technologies (ICT) companies are investing a large amount of resources. With \$1.3 billion dollars invested in Blockchain in 2018, does the current solutions and the knowledge justifies such investment or the companies are just throwing away money because it is a trending technology expecting it to be the answer to all their problems?

After understanding how Blockchain works and all the concepts related to it, it is important to see actual and possible applications of Blockchain in the real world. It is relevant to understand how Blockchain has come so far and where it possible will be in the future.

This chapter provides an overview of some use cases of Blockchain technology application in multiple areas. “The Areas for Blockchain application”, is divided into two sections. In the first (1) section, using a survey answered by key people on the Blockchain’s field, on which business areas the Blockchain will probably have more impact. The top 4 with more answers were picked and combined with it to see possible solutions.

In the second (2) section, four of today’s most relevant technologic areas (IoT, Big Data, BPM and AI) are studied. Trying to understand in which way the can be combined with Blockchain to get ideas of possible solutions with potential to help societies.

### 3.2 Business areas for Blockchain

Blockchain has an enormous disruptive potential, regarding how today's transactions work. The decentralization idea can shift the centralized structure and change the way we record and verify transactions (Frei, Wilkinson, Trepte, & Hatop, 2017).

In a Credit Suisse research of 2018, they made a survey asking business leaders in which business areas they think Blockchain will have more impact (Figure 15). From this survey, the top 4 areas with more answers were chosen for studying their viability to Blockchain (Brennan, Zelnick, Yates, & Lunn, 2018).

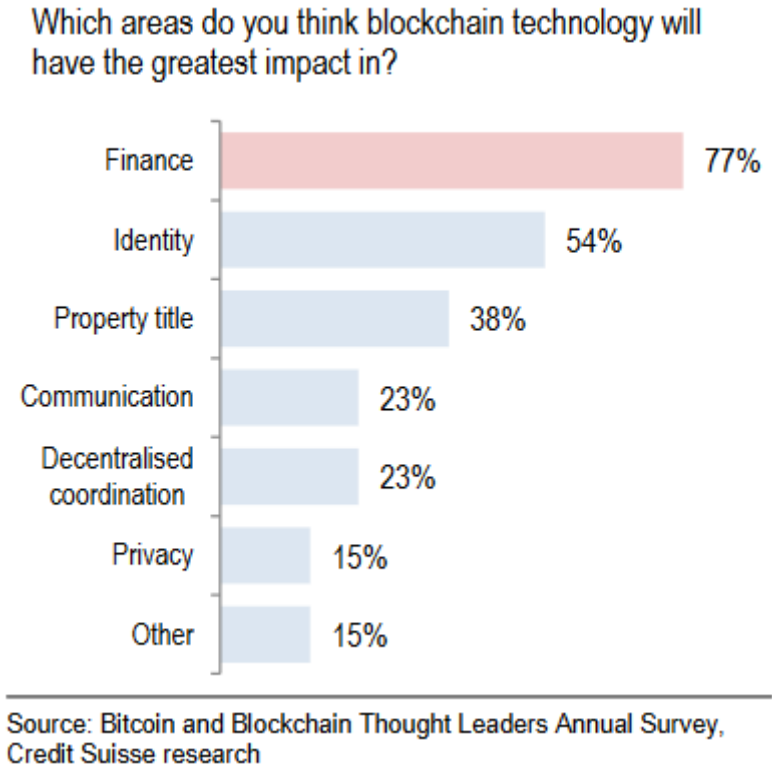


Figure 15 - Survey on Blockchain Thought Leaders

#### 3.2.1 Finance Industry

The current system relies on a high degree of trust in an environment where financial institutions record individuals' accounts in a centralized manner and banks' reserves are stored in a central bank. The Blockchain enables the creation of an 'Internet of Finance', a decentralized financial system operating on transactions. Karp noted, "A technology that has the ability to conduct and verify transactions via an immutable, time-stamped record that is replicated on servers across the globe has immense implications

*for the banking sector. We're talking about a massive overhaul of the banking industry's processes and a significant reduction in costs.*" (Karp, 2015). There are three characteristics that make this possible:

- **It's anonymous**, so it can protect the identities of users and allow entities and people to carry out transactions at never-before levels of privacy, security and non-intrusion;
- **It's permanent and digital**, so that translates into putting in any number of transactions and records in a chronological order that the whole thread or equation accomplishes degrees of transparency and credibility.
- **It's open, distributed** and can also be programmed so transactions can be triggered automatically, contracts can become set in digital code and safe from tampering or deletion ever. Every agreement between parties can, easily and non-physically, get converted into a digital record – properly identified, validated, stored, and shared. This wipes away the role, effort and expense of intermediaries, brokers, as algorithms enable fast and free interactions devoid of previous friction and oversight.

So yes, this is possible – two entities may not know each other and still agree and assign veracity to something without the presence or involvement of a third party. Blockchains can also function as 'permissioned' ledgers so that everyone in the process is pre-selected, or as 'unpermissioned' ones that are open to all (Yap, 2015).

## **Blockchain use cases in finance industry**

### **Cross border payments**

The actual banking systems have fast and secure ways for intra-country payments, however international payments can't say the same. High expenses and lack of trust with local regulation, correspondent banking has gain notoriety for cross-country settlement. But still this tool is expensive for customers and for banks that got manage with international payments. Blockchain can combine messaging and transfer of money as explained above, but for international transactions this would require an international cryptocurrency. This can improve cross border payments by speeding up and simplifying the process, while reducing costs significantly and cutting out many of the traditional middlemen. At the same time, it would make money remittances more affordable.

Santander is already using Blockchain to transfer live international payments through a mobile app. The solution uses technology provided by Ripple, the creator and developer of the Blockchain-based Ripple payment protocol and exchange network. National central banks could launch an international cryptocurrency which is backed by local currency. Although that seems far away, Polish banks have launched a cryptocurrency (in cooperation with Billon) that is backed by the zloty (Fintechnews, 2017).

### **Bank credit information systems**

Information systems of bank credit have three main problems that makes them ineffective:

- Poor quality and shortage of data are problems when deciding a personal credit for someone;
- Inter-institutional data sharing;
- Unclear ownership of user data, privacy and security becomes difficulties in circulation;

Blockchain could help organizations solve these problems, however the solution would require participation from different stakeholders (Guo & Liang, 2016).

### **3.2.2 Digital Identity Industry**

*"A digital identity contains data that uniquely describes a person or a thing but also contains information about the subject's relationships to other entities."* For example, governments store records about their citizens. These records can be anything like a VIN (vehicle identification number) that only identifies a car belonging to someone. In addition to that, it has other attributes of the car such as year, make, model and color (Windley, 2005).

### **Identity Authentication**

In our days, Internet has a great need for Blockchain based identity authentication. There are some ways to identify a person in the physical world, using Social Security numbers, drivers' licenses or passports however when it comes to online authentication of personal identities or identify digital entities there is no such thing. In some digital applications, Facebook accounts or media access control (MAC) are used as login but this system can have some flaws because they can be changed. So, while governments can issue forms of physical identification, national boundaries are not recognized by online identities and digital identity authentication seems hard to control without a global entity. It would be almost impossible, to create a global entity overseeing digital identities given that there is a common backlash against even national identity cards. Blockchain technology may be the solution because of the elimination of a central and trusted central authority (Shrier, Wu, & Pentland, 2016).

ShoCard, is a startup which is aiming for a world of digital identity which protects consumer privacy. The point is, to make a system as simple as showing a driver's license and at the same time, be secure as a bank can count on it. The key is that the ShoCard Identity Platform is built on a public Blockchain data layer so, as a company, it is not storing data or keys that could be compromised. All identity data is encrypted, hashed and stored in the Blockchain, where it cannot be tampered with or altered (SITA, 2016).

### **Government services**

Easy and fast access to government services has always been a challenge for governments, where the most important aspect is fraud prevention and thorough physical identification verification. For example, when a citizen tries to renew his driver's license typically, he must visit a physical location, identify documents in hand and go through long wait times in line so he can be attended, which can be frustrating.

With the adoption of Blockchain, services can reduce customer related costs associated with physical office space, verification and more, resulting in large amounts of money saved each year, better information sharing across the country and an improved customer service and satisfaction (Wolfond, 2017).

### **3.2.3 Property Title Industry**

The property industry moves trillions of dollars every year (PwC, 2016), especially the real estate industry, where many houses change owners every day. However, the process of selling and renting a house is still very slow and full of bureaucracies, demanding a digital transformation that can improve it. Blockchain and Smart Contracts can be a great addition to the industry because of their promises of automation and security. Blockchain can also cut the middle man, like brokers or lawyers, and cut some costs and fees that go to intermediaries.

One use case for property industry using Smart Contracts and Blockchain might be house rentals. A shared database where people who want to rent a house can see every offer. Once a client gets interested in a house, he can get information about the history of it and even contact with the owner. If both reach an agreement, Smart Contracts can handle all the money transaction and all the bureaucracy inherent to this kind of agreement. This integration could improve not only monetarily but also the speed of the process.

Other potential use case for Blockchain in Property industry, is in property title insurance. Despite many think, the cost of title insurance does not come from actual risk involved in the title but actually from the cost of personnel. By integrating Blockchain, Insurance companies can decrease the costs by a great margin by using it to store a database of accurate records which can be searched efficiently and reduce the number of defective titles that must be corrected.

Furthermore, documents can contain defects because they are not reviewed and validated by a responsible party prior to recording. If off-chain information can impact security of title, professional intermediaries will be required to perform due diligence and mitigate against risk, which is a barrier to peer-to-peer transactions. Under these circumstances, disintermediation is not desirable for the transacting parties, who would assume the risk themselves.

### **3.2.4 Communication Industry**

Online communication faces many challenges, one of them, is creating a secure way of connecting and creating relations between people while creating a secure environment without worrying about identities and personal information. People need places to access and share ideas with equal opportunities without being continuously monitored. Blockchain might have the tools to fight these problems (Skrumble Network, 2018).

#### **Publiq**

Publiq is a distributed network using Blockchain that was born to revolutionize the media industry. Online media is rapidly growing where no exchange exists, Publiq promises to change the way people interact and stay up-to-date. There are 3 types of users in this network, authors, channels and readers. The process begins when an author creates and publish his article into the network. The article then becomes available in two ways:

- On the Publiq interface where every article published in the network can be found
- On the channels that decide which content they want to broadcast

The point of the channels is to distribute and promote the content they think are more appropriate for them. They can choose which articles they want to show to their readers, however, the articles not picked by them are still available to the readers through the first way, preventing censorship. By promoting the article posted in the Publiq, depending on how much traffic a channel generates, they can be rewarded. Once the post gets to the reader, after reading he can evaluate it by liking, sharing or flagging



the article. This way, an author can get a score based on the articles he wrote and consequently the higher the score the more consideration he gets. A platform for promoting and sharing news/articles based on Blockchain can inherit the security of encryption and sharing of a peer-to-peer network. Integrating Smart Contracts with it can help fighting against mass likes and sharing from bots with the intention of boosting articles (Publiq, 2017).

## **Mavin**

With the growth of social media, many opportunities came with it. Social media give people and organizations major exposure to the others. Some people started to gain fame through it exclusively by posting content made by them and viewers liking it and following it. These content creators are called influencers and because of all the fan base they have organizations look at them as a way of marketing for their business. Mavin combines this new “business” and combines it with Blockchain.

There are two main roles in the platform, influencers and marketers. In Mavin’s platform, anyone can be an influencer, even the smaller ones, so everyone can get paid according to the traffic and media mentions they generate. Marketers use Marvin to reach the influencers and paid them to help promote their products. A person with a group of followers recommending a product can have a major impact instead of a TV star advertising. There is also a role for human verifiers that help to ensure quality in the platform and earn money for his work. Blockchain technology, in this use case, makes the micro-payments 10-times cheaper than traditional micro-payments, allowing instant payment by cryptocurrency to influencers (Mavin, 2018).

## **3.3 Technologic areas for Blockchain**

### **3.3.1 IoT**

*“Internet of Things (IoT), also known as the Internet of Objects, is a foundation for connecting things, sensors, actuators, and other smart technologies, thus enabling person-to-object and object-to-object communications.”* (Kuyoro, Osisanwo, & Akinsowon, 2015).

Proposed in the end of the 1990’s by MIT Auto-ID Labs (Auto-ID Labs, 1999), the primary purpose of IoT is to share information about objects, which reflects the manufacture, transportation, consumption and other details of people’s life. It has three important characteristics (Ma, 2011):

- Any objects can be instrumented. Objects like chairs, doors, foods can be embedded with a chip, bar code, etc., and then we can address them;
- Autonomic terminals are interconnected, acting like autonomic network terminals;
- Pervasive services are intelligent. In such an extensively-interconnected network, letting every object participate in the service flow to make the pervasive service intelligent. For example, the sensor nodes of vehicle-carrying network or human-carrying network can monitor the status of road or the body of driver to obtain real-time information for guiding driving behaviors.

Despite all the potential the technology has, it still has some challenges. In relation to security, IoT endpoints are opening vulnerabilities for systems around the world. There are stories of these endpoints being hacked and that creates a real threat to the technology.

Most businesses have built their infrastructure for the internet age. The architecture is designed with the idea of dealing with online connections and interactivity. But even for large businesses, the predominant architecture is a centralized model. Companies authenticate, authorize and connect with their users from a central infrastructure. The issues of scalability are addressed in terms of adding and subtracting resources from a central pool. The problem with IoT is that there are going to be too many of them to make the centralized model work.

Businesses will have to adapt to decentralized architectures to deal with the onslaught of IoT devices. Companies must update their systems to cope with large amounts of data that the IoT devices will produce. They will need to study and understand the challenges of decentralized connectivity models.

IoT is not a new concept. Manufacturing and other industries have been using different connected devices like sensors, scanners, and cameras for a long time. Over time each manufacturer has developed their own machine-to-machine (M2M) protocols. But the lack of standardization poses a huge problem for IoT. Multitudes of M2M communication protocols can make it difficult to integrate products and services across different brands.

Developing a common protocol to work across different manufacturers and brands is in the best interest of both the producers and consumers of IoT. Everyone involved with IoT should put serious effort to create more common protocols and infrastructure for the connected devices to communicate with each other.

## **Examples of Blockchain and Smart Contracts incorporating IoT**

- **Seafood (Supply Chain Traceability)**

Currently in the traditional fish business, there is a lot of problems, i.e., fishing practices are illegal, unregulated or unreported; after being caught the fish get labels not corresponding to them (seafood fraud) and when it is stored the material may be in improper conditions. All this lack of proper business management has impacts in the consumer's final product quality and there is no way for the consumer to know, creating a lack of vendor and consumer trust.

To prevent these problems, combining IoT, Blockchain and Smart Contracts could be the solution. Recording the trip of all sea-food since when it was fished from the sea until it gets to the final consumer. IoT sensors can be attached to any object entrusted to someone else for transport, with trackable ownership, possession, and telemetry parameters such as location, temperature, humidity, motion, shock and tilt. The final buyer can access a complete record of information and trust that the information is accurate and complete (Hyperledger, 2016).

- **AutoPay**

Marie goes to work in her car. As soon as she enters the car, it synchronizes with Marie's smart phone's AutoPay service. This service gives security and trust to Jane through Smart Contracts on its Blockchain interface, acting as a device for autonomous payments. AutoPay defines her office as her destination. The service interrogates the vehicle data about his fuel and if is low automatically finds a route which passes by a petrol station that is advertising competitive fuel price. After refueling the car, which was automatically paid by AutoPay's Smart Contract feature, Marie receives a message telling her that her work's car park is full and AutoPay, through Smart Contracts, paid for another car park, very close to her office.

After work Marie goes home, and her daughter Ana asks to borrow her car. Ana's Smart Contract allows her to access her mother's car but don't let her make autonomous payments for everything. So, every member of the family has different Smart Contracts which have certain conditions according to their role in the family. Ana can refuel using her mother's AutoPay service, but she can't use it on McDonald's drive through to buy meals for her friends because those conditions are not present in the Smart Contract. If still there was a way for Ana to pay for things she should not, Jane could easily find out because of the

immutable transaction history she has access to on AutoPay's interface to the car's Blockchain's ledger (Huckle, Bhattacharya, White, & Beloff, 2016).

- **Smart City – Smart Homes**

There is a panoply of household devices present in today's houses. Sensors to control the environment, refrigerators, dishwashers, cameras, door locks, alarms many of them are IoT devices. Homeowners or authorized parties can have access to these devices to control the smart home. All the information coming from these devices is stored in a central server and then its presented to the controller in devices like a cell phone or a computer. This information cannot end up in other hands besides authorized person so maintaining the security is very important and Blockchain can help in that field. Making use of distributed ledgers, the communication and control information can be recorded as transactions. Using symmetric cryptography to maintain confidentiality, hashing functions to maintain integrity and asymmetric cryptography for authenticity, a robust security can be ensured. Attempts to corrupt the system could be immediately detected. A DDoS (Distributed Denial-of-Service) could be easily stop because of transactions between nodes can be verified and any unauthorized transaction can be rejected (Hussain, Ferworn, & Zahid, 2017).

### **3.3.2 BigData**

*"Big data is generated from an increasing plurality of sources, including Internet clicks, mobile transactions, user-generated content, and social media as well as purposefully generated content through sensor networks or business transactions such as sales queries and purchase transactions. These data require the use of powerful computational technologies to unveil trends and patterns within and between these extremely large socioeconomic datasets."* (George, Haas, & Pentland, 2014).

In bigger organizations, databases can go up to Petabytes, so companies need to guarantee that all the data centers are synchronized in real time and all the data is authentic. Besides, companies need to protect these data from unauthorized people trying to access it. These challenges can be mitigated with the help of Blockchain because of three essential properties (Sharma, 2018):

- Decentralization – As data storage and management is decentralized this helps increasing the security. If some person tries to compromise or corrupt the data, decentralization guarantees copies of the data that have not been modified in a malicious way. If a group of people tries an organized attack on the data, they would need to be in control of most of the network, which is a very hard task.

- Data immutability and integrity – Immutability on data is a very important aspect for corporations that are interested in Big Data. If a dataset that needs to be studied is modified, the analysis from it will not add value to the company because the data is not the real one. Also, companies need to be sure the information gathered is coming from an authentic source to make a real analysis.

## **Examples of Blockchain and Smart Contracts incorporating Big Data**

### **Health Industry**

There is a great potential for Big Data in the Health industry. Clinical trials, electronic records, patient databases, medical measurements, etc., produces many data in different formats and from different data streams. To take advantage from all this information it is necessary to interpret it in a quick and efficient way. Thus, new tools are required to track, trace and provide fast feedback for individual patients. Interventions and health services will be easier to predict with the help of a proper data management. Medicine evolves while introducing new technologies, so it is always important to look to innovations and try to implement them in this area. As new tools are needed to deal with healthcare data, Blockchain can take this role. So, Blockchain has clearly a potential to help deliver this concept. As data would be stored with the latest secure technology and using verifiable cryptography, patients can have full control on their records, so they can decide when to share it (Raghupathi & Raghupathi, 2014).

### **Financial Industry**

Blockchain combined with Big Data can bring many benefits to Financial Industry, in the field of analytics. As data stored in Blockchain has the promised of being secured relatively to forging and corruption, this data can be used for analysis purposes. Also, the data is structured making it good for analysis. For example, a Blockchain network that allows financial institutions check all the transactions happening in real time. Once a transaction happens, the bank could analyze it in real time and see if there was any fraud involved. As for the current system, where the fraud prevention is made by analyzing all the records of the fraud.

### **3.3.3 BPM**

*“Business Process Management (BPM) is the art and science of overseeing how work is performed in an organization to ensure consistent outcomes and to take advantage of improvement opportunities.”*  
(Dumas, Rosa, Mendling, & Reijers, 2013).

Depending on the objectives of the organization, improvement can come in different ways. Some organizations use BPM to reduce costs, others to reduce error rates. With these benefits, organizations try to increase competitiveness and sustainability in times of market uncertainty whose business conditions are constantly changing. Organizations need to shift to process-centric thinking (Doebeli, Fisher, Gapp, & Sanzogni, 2011) , they need to improve organizational performance in ways they know. They need to look to the big picture and know an improvement was achieved and is being sustained, not guessing but knowing (Tregear, 2011).

### BPM Six Core Elements and Blockchain

Each of the six core elements represent a critical success factor for Business Process Management. Therefore, each element, sooner or later, needs to be considered by organizations striving for success with BPM (Figure 16).

Strategic Alignment	Governance	Methods	Information Technology	People	Culture	Factors
Process Improvement Planning	Process Management Decision Making	Process Design & Modelling	Process Design & Modelling	Process Skills & Expertise	Responsiveness to Process Change	Capability Areas
Strategy & Process Capability Linkage	Process Roles and Responsibilities	Process Implementation & Execution	Process Implementation & Execution	Process Management Knowledge	Process Values & Beliefs	
Enterprise Process Architecture	Process Metrics & Performance Linkage	Process Monitoring & Control	Process Monitoring & Control	Process Education	Process Attitudes & Behaviors	
Process Measures	Process Related Standards	Process Improvement & Innovation	Process Improvement & Innovation	Process Collaboration	Leadership Attention to Process	
Process Customers & Stakeholders	Process Management Compliance	Process Program & Project Management	Process Program & Project Management	Process Management Leaders	Process Management Social Networks	

Figure 16 - BPM Six Core Elements

### Strategic Alignment

Organizational strategy is the sum of the actions a company intends to take to achieve long-term goals and BPM needs to be aligned with it. Strategic alignment is a “connection” between organizational processes and priorities enabling continuous and effective action to improve business performance. Processes must be designed, executed, managed, and measured according to strategic priorities and specific strategic situations. With the use of strategic alignment organizations can look to their longevity and find how possible is to get their visions for the future (Morrison, Ghose, Dam, Hinge, & Hoesch-Klohe, 2011).

For an organization to take advantage of Blockchain technology regarding strategic alignment, it needs to:

- First, when defining a strategic position companies need to consider Blockchain technology, so can processes be aligned with this position. Thus, organizations need to research how the impact of the technology on specific processes can be systematically analyzed. They need to look which processes would improve with the introduction of the technology, which strategies would appear with Blockchain;
- Second, Blockchain changes the process-follows-strategy paradigm with the Blockchain-based processes challenging entire industries. For many companies, the elimination of the middle men by the Blockchain could harm the banking industry instead of helping.

## **Governance**

BPM governance establishes appropriate and transparent accountability in terms of roles and responsibilities for different levels of BPM (portfolio, program, project, and operations). A further focus is on the design of decision-making and reward processes to guide process-related actions. Comprises a variety of mechanisms that may be impersonal (e.g., laws or rules) or personal (i.e., administered by individuals who may or may not have formally designated responsibility or accountability for governance) (Vom Brocke & Rosemann, 2010)

In terms of governance, Blockchain has the following implications:

- Connecting dedicated roles with internal and external partners for setting up Blockchain support for processes
- Policies to rule when and where Blockchain technology can be used or can't be used for supporting processes. In cryptocurrencies, their value shifts multiple times and can be a high difference between values. But for private and consortium-based Blockchains it is not so exchange rate is not so important because there will be no sudden influx of new capital without authorization and the common ledger will be used for shared processes and data.

## **Methods**

This core element talks about the techniques and tools used to support and enable actions about processes, in each level of the process lifecycle. Process modeling and analysis are examples of methods (Plattfaut, Niehaves, Pöppelbuß, & Becker, 2011).

Blockchains may affect methods in the following two ways:

- Using Blockchain for processes have benefits, costs and risks associated and it is needed to use specific novel analysis methods to see the impacts;
- Specific engineering methods are required for specific features of Blockchain technology and its usage in supporting inter-organizational processes. There is a need for formal reasoning capabilities about the correctness and privacy preservation of processes that are designed based on Smart Contracts.

## **Information Technology**

Information technology corresponds to software, hardware and information systems who makes business processes possible. IT solutions usually have an explicit understanding of the process and what needs to be executed (Vom Brocke & Rosemann, 2010).

Blockchain technology enables novel ways of process execution, but several challenges must be considered:

- The implementation of Blockchain requires new software components and integrated development environments;
- Security and privacy are always an important factor for organizations to prevent any data from ending in the wrong hands. Blockchain has restricted vision of encrypted data and every node need to ensure that the confidentiality requirements are met.

## **People**

People define all individuals and groups (human resources) who participate in the organization's processes in order to improve business performance. The organization needs to develop the workforce to be BPM-ready. This factor shows how capable the human capital is in an organization (Vom Brocke & Rosemann, 2010).



As Blockchain is a new technology, there is a need for qualify workers with skill sets to work with it. These skills are, contract management, software engineering and cryptography. Transforming processes into Smart Contracts require new ways of thinking since actors in inter-organizational processes are freer to act than intra-organizational process participants. The openness of Blockchains makes easier for other organizations participate in ongoing processes (Plattfaut, Niehaves, Pöppelbuß, & Becker, 2011).

## **Culture**

Culture refers to collective values, beliefs, soft factors or behaviors and attitudes towards business process. Impact of culture has a great importance in the success of an organization. This is about creating a facilitating environment that complements the various BPM initiatives and the culture of an organization needs to foster the development of both business processes and business process management (Milani, García-Bánuelos, & Dumas, 2016).

Blockchains probably is going to make an organizational culture move to a stronger flexibility and looking into another perspective around the organization. In the competing values framework by Cameron & Quinn, these aspects are associated with an adhocracy organizational culture. Furthermore, not only consequences of Blockchain adoption must be studied, but also antecedents (Cameron & Quinn, 2011). These include organizational factors that facilitate early and successful adoption.

### **3.3.4 AI**

Across the years, AI (Artificial Intelligence) received many different definitions according to different perspectives. Bellman defined AI as *"[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning..."*. As for Kurzweil, AI is *"The art of creating machines that perform functions that require intelligence when performed by people."* Winston sees AI as *"The study of the computations that make it possible to perceive, reason, and act."* (Russell & Norvig, 2016).

So basically, AI is *"Software that makes it possible for machines to make decisions more autonomously and efficiently. Artificial Intelligence uses enormous amounts of data to glean knowledge of how decisions are made to learn to replicate those modes of deciding. Essentially, AI aims to create machines that can operate without human supervision."* (Sharma, 2018)

How can Blockchain help AI? The main goals of a Blockchain is a constant update of all the data stored and this data is very secure because of the cryptography used by it. While AI tries to achieve the

best decision, it can use the data stored from the Blockchain and get better results with highly reliable information.

### **Prediction market**

Augur is a decentralized Blockchain-based prediction market where a result from an event can be predicted using the “wisdom of the crowd” principle. In this concept, information gathered from the crowd is averaged into the most realistic possibility and get the most probable result. Those who have right predictions get rewards by the network, while wrong predictions have losses. Decentralization helps Augur to not be censored by governments that deem prediction markets as gambling, also helps fighting against fraud because of the honesty of the reports are always ensured (Peterson, Krug, Zoltu, Williams, & Alexander, 2018).

### **Handling huge amounts of data**

In this information era, lots of data are continuously being created. Only on the internet, users generate many quintillion bytes of data each day and to normalize all this data is very hard. AI could normalize this data and made it available into the Blockchain, where it would become less prone to corruption to hackers because of the decentralized storage across the network. Even in natural catastrophes, the data will always be secured because every node has a copy.

### **Decision making**

As explained before, Proof of Work (PoW) consists in multiple miners trying to solve algorithms to find the best solution and once found the block is sent to all nodes. AI works in the same idea, to take a decision the machine analyses every possible solution until it finds the best under a certain condition. This process requires a lot of computational power and if the decision is very complex it could take some time. Combining AI with Blockchain, all the nodes present in the network could participate in the task of taking a decision. This way, the process would be divided to everyone and it would take less time.

### 3.4 Conclusion

*“Everything will be tokenized and connected by a Blockchain one day” – Fred Ehrsam*

After elaborating this chapter, it is possible to claim that besides the major success of the technology in the financial area, its potential is much wider to only focus in cryptocurrency. The transparency and immutability, which are inherent to this technology, bring also benefits in other areas.

One interesting use case is house rentals. A shared database where people who want to rent a house can see every offer. Once a client gets interested in a house, he can get information about the history of it and even contact with the owner. If both reach an agreement, Smart Contracts can handle all the money transaction and all the bureaucracy inherent to this kind of agreement. This integration could improve not only monetarily but also the speed of the process.

Other interesting use case is Seafood (Supply Chain Traceability). Currently in the traditional fish business, there is a lot of problems, i.e., fishing practices are illegal, unregulated or unreported; after being caught the fish get label not corresponding to him (Seafood fraud) and when is stored, the process may be in improper conditions. All this way of business management has impacts in the consumer's final product quality and there is no way for the consumer to know, creating a lack of vendor and consumer trust. All data related to the phases of production, packing and transportation can be inserted into a Blockchain where the user can have access to all the conditions his product went through. All this potential together with Smart Contracts allow to create a system totally reliable where third parties can have a major network between them without worrying about security.

Besides all these use cases about Blockchain and Smart Contracts, is important to analyze each case and see if it does really make sense the introduction of these technologies. Many new solutions use these technologies only because they are trending, and the same work can be done with technologies used before. Each case is a different case and it is necessary to do a careful analysis, evaluate the pros and cons and see if the introduction of these technologies will add value to the solution.



## 4. The Insurance Domain

### 4.1 Introduction

*“Insurance - an ingenious modern game of chance in which the player is permitted to enjoy the comfortable conviction that he is beating the man who keeps the table.” – Ambrose Bierce*

The objective of this chapter is to understand a little bit more about the business area where the Blockchain solution will be implemented. The Insurance domain is an area always expanding, with a high number of processes which have a lot of bureaucracy and data produced. In the specific case of car insurance, this is since nowadays, there is a law that force every car to have an insurance. In 2016, in Portugal, it was estimated that about 4.850 million light passenger vehicles were in circulation (PORDATA, 2016). This means that there were 4.850 million car insurances. In other words, many records to be stored and many paperwork to be made.

Even so, it is not only the paper work and stored records that bring headaches to the insurance companies. Fraud is also a problem that costs them a lot of money, and it is very hard to fight some fraud situations without insurance companies working together. For these reasons, it is possible that Blockchain technology may be used to develop a more sustainable and viable solutions to help insurance companies dealing with processes.

This way it is important to study a bit of the insurance activity, with the purpose to find and understand which problematic situations may exist in the insurance sector, particularly in the case of car insurance.

## 4.2 Insurance History

In Pre-History, families were organized into tribes and forms of cooperation and solidarity were already present among the members of the tribe. When a misfortune happened the consequences of the damages were distributed among to mitigate the loss of the victims.

In the hype of the Old China (5000 a 2300 A.C.), the transportation in rivers was made in fragile boats. Cautiously each boat transported only a small part of the merchandise of each merchant. In case of sinking or robbery only a part of the goods of each one was lost. This ancient way of prevention consists in the fragmentation or distribution of the risk to minimize the losses if something happens. Still today this process is used (Swiss Re, 2014).

In 1293, the King D. Dinis established in Portugal the first form of insurance, dedicated exclusively to the sea risks. An agreement was reached with merchants, aiming for the payment of certain amounts according to the boats and their traffic. These sums of money were there to face the accident of losing ships or merchandise. The first laws about it in Portugal are enacted in 1370, and the first law is for cargo ships weighing more than 50 tons, which were obligated to be registered. This is the date of the first Reinsurance (Diffie & Winius, 1977).

In 1666, in London there was a great fire who destroyed a major part of the city. Houses, many churches, St. Paul Cathedral and public buildings were destroyed, however few people died. Hardly any of the destroyed homes were insured and this changed public opinion about insurances (Swiss Re, 2013).

The industrial revolution and the growth of the British Empire called for insurance solutions. Towards the end of the 18<sup>th</sup> century the first truly modern and global insurance company, the Phoenix, was founded by an association of sugar refinery owners in London. In India, insurances were restricted only to British subjects as locals were suspected of not being morally fit to withstand the temptations of fraud. Ironically, the worst risk for life insurers turned out to be young British officers who were often exposed to severe health problems in the tropical climates of the colonies and tended to die prematurely (i2S, 2012).

In 1845, in Germany was created the Reinsurance Cologne company (Swiss Re, 2013). This company created insurance of agricultural, personal accidents, work accidents, car, livestock mortality and many others.

So nowadays, insurance is basically, a contract between an insurer and an insured. In a contract, the insurer indemnifies the insured against losses, damages, or liability from an unknown event. A

preexisting condition must not exist for insurance to be valid. For example, obtaining automobile insurance after an accident is not insurance and does not indemnify the insured for any injuries suffered.

### **4.3 Car Insurance**

The car insurance is present in the 128.º article, al. b) of Law n.º 94.º-B/98, of 17<sup>th</sup> April (Ministério das Finanças, 1998) and the obligatory for having an insurance of motor vehicle is regulated by DL n.º 291/2007, of 21<sup>th</sup> of August (Ministério das Finanças e da Administração Pública, 2007). Car insurance, in case of, for instance, a traffic accident, aims to protect the victim's interest, independently if the responsible for the accident has or not the economic conditions to indemnify for the damages. The vehicle who has no insurance, finds itself in illegal situation, can be apprehended and its owner can pay a fine for it.

The truth is, the insurances companies aren't obligated to accept insuring a vehicle, even if it is an insurance of motor vehicle liability. However, those who can't arrange an insurance after contacting at least 3 companies, should ask a declaration of deny (art. 2.º from the Regulatory Norm n.º 9/2006-R) (Instituto de Seguros de Portugal, 2006), to posteriorly, contact the Portuguese Insurance Institute, and show those declarations as well as the required documentation. The Institute will define which insurance company have to accept the insurance and which price will be charged (article 3.º, n.º2 from Regulatory Norm and art. 18.º from DL n.º 291/2007, of 21<sup>th</sup> of August) (Ministério das Finanças e da Administração Pública, 2007).

The motor vehicle liability insurance covers accidents inside the borders in which the national services of insurances have an agreement between national services and the accidents occurred on the path which directly connects the two territories where the agreement of European Economic Space is applied, not existing in it the national service of insurances (art. 10.º DL n.º 291/2007, of 21<sup>th</sup> August) (Ministério das Finanças e da Administração Pública, 2007).

The obligated insurance covers the payment of indemnifications for corporal damages of materials caused to others and the passengers, with exception of the driver, as said in art. 14.º, n.º 1 (Ministério das Finanças e da Administração Pública, 2007).

Very often people use the expression "insurance against all risks", however, the truth is there is no insurance against all risks. This expression usually is used to designate insurances which cover one's own damages, covering damages suffered by the vehicle insurer even when the driver has guilt in the accident.

## **Insurance Policy**

Insurance Policy is a set of documents issued by the Insurer, which has conditions to regulate and formalize initially the insurance's contract. It should have (Ministério das Finanças e da Administração Pública, 2008):

- Date;
- Identification and signature of the insurer;
- Identification of the client;
- Object of insurance, its nature and value;
- Covered Risks;
- Start and expiration date of the contract;
- Initial and subsequent premium;
- Method of payment of the premium;
- All circumstances of interest to the insurer relating to the risk;

## **Insurance Cessation**

Insurance's contract ends in general terms, namely by Expiration, Revocation, Denunciation and Resolution. Without prejudice to provisions establishing the effectiveness of contractual obligations after the term of the bond, the cessation of the contract determines extinction of insurer's obligations and insurance client. The cessation of the contract does not prejudice the obligation of the insurer of performing a provision due to the risk cover, as long as the accident is previous or concomitant with the cessation even though it is the cause for cessation of the contract (Ministério das Finanças e da Administração Pública, 2008).

## **4.4 Frauds**

Insurance fraud is one of the most common fraud in the world, losing only for tax fraud. Since the creation of insurances, it has always been very vulnerable to fraud because people are always open to make schemes where they can make easy money (Whitaker, 2018).

### **What is Insurance Fraud?**

Insurance fraud happens when the client tries to profit by violating the terms of the insurance contract. Fraudulent people create losses or do damages in their property rather than acting like normal people who have no losses but want to preclude in case of something happens.



A Fraud can happen in any phase of insurance life cycle:

- Individuals applying for insurance
- Policyholders
- Third-party claimants
- Professionals who provide services to claimants

There are two forms of insurance fraud: hard frauds and soft frauds. Hard fraud is when an accident is made on purpose to steal money from the insurance company. Soft fraud is when an accident occurs naturally without intention of making it, but the insured add something more to the claim that have nothing to do with the accident to gain more from it. The claim is made exaggerated (Whitaker, 2018).

### **Impact of Insurance Fraud**

Insurance fraud has a major impact in the insurance companies profit and consequently this increase the cost the consumer pays to have an insurance. The losses for fraudulent claims can only be estimated because usually fraud is only discovered when the schemer starts to be greedy and the fraud scheme becomes obvious for the company, so many claims can go through without anyone seeing it has a fraud. Insurance frauds can be made by any person and the only thing necessary is only to have an insurance. Plus, what makes insurance fraud hard to fight is that authorities usually don't have the expertise to perform a good investigation in this sector. So, for this, insurance companies need to train their staff to identify the evidences of insurance fraud schemes.

### **Vehicle Insurance Schemes**

- **Ditching**

This scheme happens when the owner abandons his vehicle with the intention of it being stolen or stripped for parts. They point of this is to make some money from the insurance policy or to settle an outstanding loan. Many times, the vehicle is expensive and purchased with a small down payment (Whitaker, 2013).

- **Past Posting**

This happens when a person, without an insurance in his vehicle, has an accident. He then makes an insurance for the damaged vehicle and waits some time. Reports the accident and pretends that it happened during the time the vehicle is covered by the insurance (Whitaker, 2013).

- **Vehicle Repair**

Consists on billing new parts for the vehicle but instead use old or not original equipment parts to repair it. The new parts can be resold to gain additional money (Whitaker, 2013).

- **Vehicle Smuggling**

In this case, the client buys a new vehicle using his maximum financing. A counterfeit certificate can be used to insure to the maximum the vehicle, proving its free and clear. Its then shipped to a foreign country and reported stolen. Once in the foreign country the car is sold, and the criminal can collect the insurance for the theft (Whitaker, 2018).

- **Phantom Vehicles**

To prove if a person is the owner of a vehicle, a document called “certificate of title” is used. Although this document doesn’t prove 100% that a vehicle exists, it is used by the insurance companies as a support insurance policy. By this reason, collecting on a phantom vehicle has been shown to be easy to do (Whitaker, 2018).

- **Cash for Crash**

This scam happens when the criminals intentionally make the drivers to crash into their cars and then blame the victim. An example scenario of this scheme is when a driver is waiting to enter a roundabout and there is a car in front of him. A driver behind the first car sees nothing is coming and its ok to move forward. The car in front gets the same conclusion and decides to go but suddenly breaks for no reason and consequently the car behind ends up hitting the other. Theoretically this seems a normal accident, but it’s all staged by the criminals (Nolan, 2014).

- **Double Dipping**

Double dipping consists in claiming the same accident to multiple insurance companies and with this gain more money for the same loss. In auto insurance context, double dipping consists in filling a claim with two different insurance companies. An example of this is when a person has a health insurance from a company A and an auto liability insurance from company B. When he has an accident, if he activates both insurances for the same accident can be seen has wrong because he would get a pay-out from both companies gaining twice for the same thing (Johnston, 2008). This fraud is going to be the use case for the Blockchain solution developed in this work.

## 4.5 Conclusion

*"Fraud is the daughter of greed." – Jonathan Gash*

Insurance has come a long way since its creation, in China, when each boat transported only a small part of the merchandise from each merchant. In case of sinking or robbery only a part of the goods of each one was lost. This ancient way of prevention consists in the fragmentation or distribution of the risk to minimize the losses if something happens. Since then, insurances have a major importance in our society. In car insurance, people are required by the terms of the art. 4.º of DL n.º 291/2007, of 21th of August (Ministério das Finanças e da Administração Pública, 2007), to make an insurance for their car. This way, when an accident happens, independently if the responsible for the accident has or not the economic conditions to indemnify for the damages, the victim's interest is always preserved. The vehicle who has no insurance, finds itself in illegal situation, can be apprehended and its owner can pay a fine for it.

Despite being a great idea, it still has many flaws. One of them is fraud and it might be as old as insurances. People are always trying to find new ways of breaking the law and gain some easy money from insurances, that is the reason that there are so many types of frauds. With the advances in technologies many frauds can be prevented, and Blockchain and Smart Contracts can be the answer to end some of them. Everything related to personal data that are used upon making insurances can be verified by Smart Contracts, stored in a Blockchain and accessed when needed. This way, insurance companies know this information is reliable and people don't need to worry about their data because of the use of private and public keys.

Besides fighting the frauds problem, Information and Communication Technologies have proven over the past years to perform a major role in companies. Many processes in Insurance Companies require a lot of paperwork, time and money. Blockchain and Smart Contracts can also help companies in these drawbacks. As already known, Smart Contracts have the automaticity and the security of physical contracts without the need of a notary. All that combined with the immutability and security of Blockchain have all the promises to be very important in Insurance area.



## 5. Blockchain Demonstration Case

### 5.1 Introduction

*“Experience serves not only to confirm theory, but differs from it without disturbing it, it leads to new truths which theory only has not been able to reach.” - Dalember*

After understanding the concepts and areas to implement Blockchain, the aim of this chapter is select a problem which might benefit from the characteristics of Blockchain and create a solution for that problem. In this case, we would like to solve a problem outside the financial sector, which was the ground where Blockchain was born and grew up. As the last chapter suggested, the area of interest is Insurances, because it has a lot of problems related to frauds and we feel that Blockchain might have a major role in fighting fraudulent situations.

This chapter is divided into 3 main sections. In the first section, is shown how an “As Is” and a “To Be” situations of what would change with the implementation of Blockchain and an architecture of how the solution would be are described. The second section is a list of all tools used to develop the solution. And the last section shows how the solution works and how all the processes go. The main processes are: Creation of an Insurance, Creation of claims, End of an Insurance and Check the history of a car (how many insurances and claims it had during its lifetime).

## 5.2 Architecture and Business Process

Nowadays, the most widely used architecture for the development of distributed systems is known as client-server. For the communication to occur between clients and servers, there are some standardized protocols to support it, for instance, HTTP or FTP (See Figure 17).

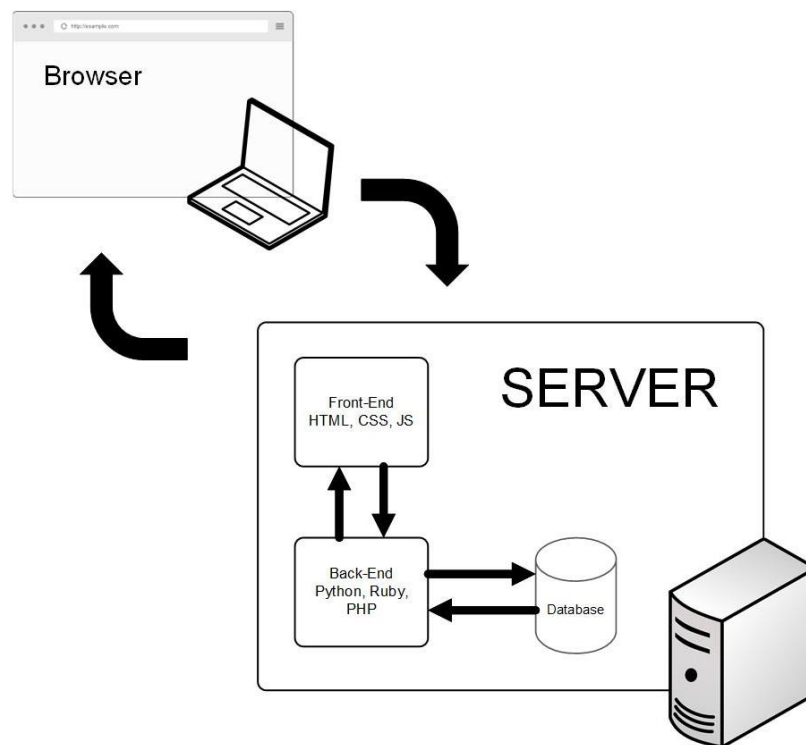


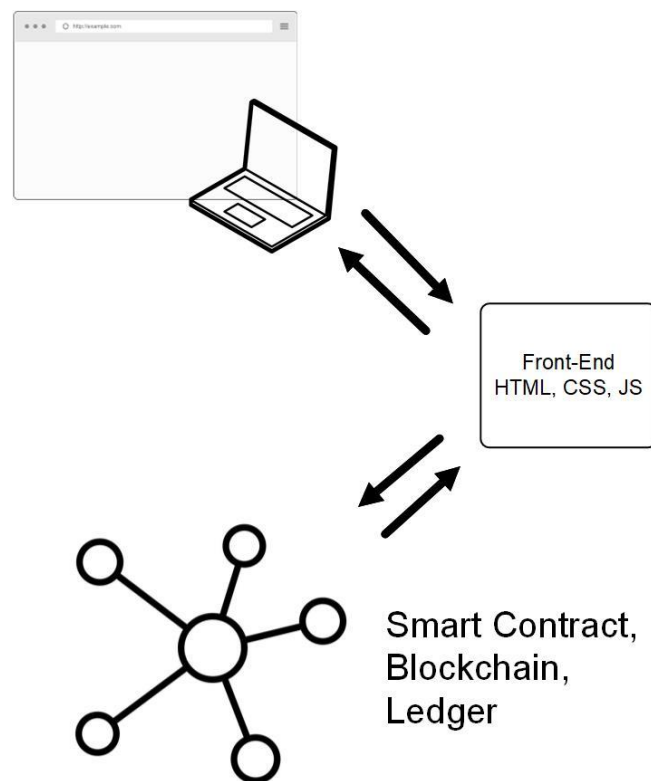
Figure 17 - Client Server architecture (Adapted from: <http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial/>)

In this architecture, the Client has an interface for users to request services of the Server and show the results from that request to the user. Servers are always waiting for requests sent by the Clients and once they arrive, they automatically do the necessary processing and send back the responses. This model is very effective when both, Server and Client, have different tasks each other. The Client does not need to know anything related to the specifics of the system of the Server. For example, in a hospital, a Client can have an application which handles with patient information and the Server has a program that handles the database in which patient data is stored (Oluwatosin, 2014).

So, in this architecture, when a user uses a browser to interact online with an application, all the requests made are sent to a central server. The application and all the data present in the database are stored in that central server. If the Insurance support system was to be built this way, there would be a few problems:

1. This server has an important role for the system work and because of that it also is a major point of failure, if the server goes down the system goes down as well;
2. The data present in the database can be changed/removed.

Having all these implications in mind it is good to look to new ways of mitigating these problems and Blockchain could be one of the ways. Building an application on the Blockchain, in which everyone is connected to everybody through the network, can help eliminating the first problem. As for the securing the data, Blockchain is very strong on that field because of the consensus mechanism insuring nothing is changed/removed (See Figure 18).



*Figure 18 - Solution based on Blockchain (Adapted from: <http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial>)*

Instead of the usually central server with a database, Blockchain can be a network and a database combined. The data present in the network can be available to all the companies because of its peer-to-peer capabilities. Every company has a copy of the data and code present in the Blockchain. There is no more a single point of failure compromising the entire network, just multiple computers interacting with each other in the same network.

## AS IS

Making an insurance today is faster and more efficient than a few years ago. Insurance companies are always looking into Information Technologies for new ways of helping them improve their business processes, as well as fighting frauds.

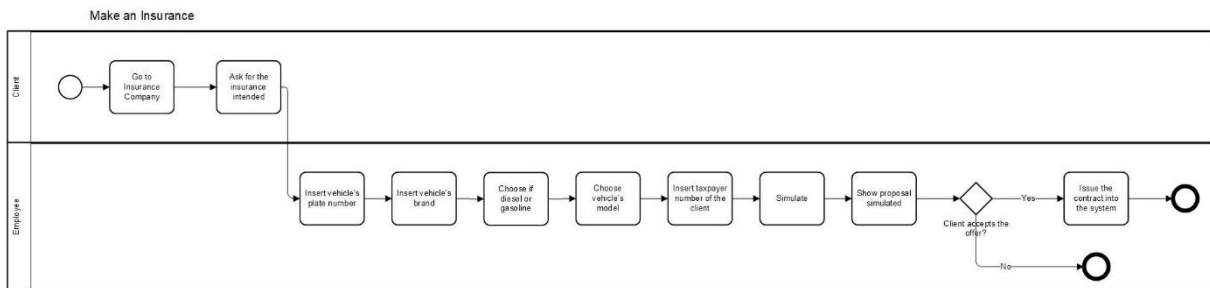


Figure 19 - Car insurance creation process "AS IS"

For example, purposes, a simple process of making an insurance is considered (Figure 19). The client goes to the insurance company with the intention of making an insurance of his car. Once there he talks to the insurance mediator about the deal. The insurance mediator asks for all the required information, for instance, car plate, characteristics of the car and client's age. After inserting that information into the system, it makes deal suggestions for the mediator to purpose to the client. If the client accepts, the insurance is submitted into the system, otherwise nothing happens, and deal is not made.

## TO BE

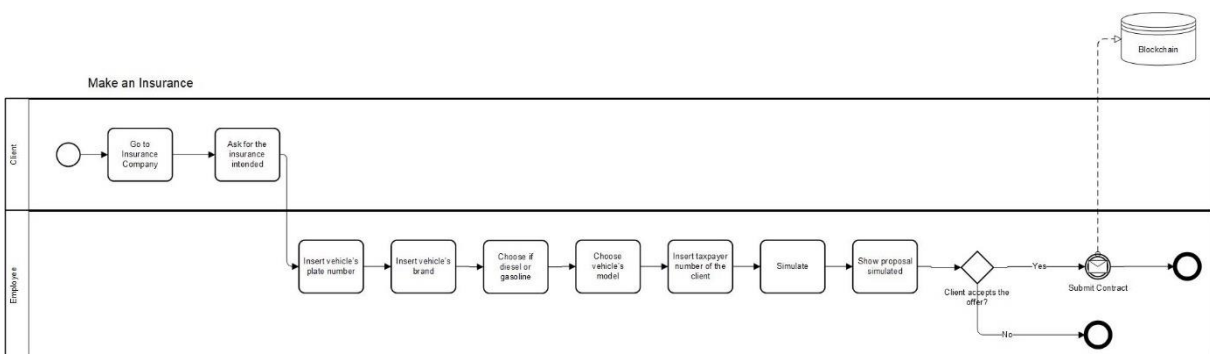


Figure 20 - Car insurance creation with Blockchain "TO BE"

With the integration of the Blockchain into the business process, most of the parts of the process would still be the same with the difference when submitting the contract to the system. After the client accepts the terms, the mediator submits the contract into the Blockchain and a Smart Contract will automatically be activated. Purpose: To verify if the car has already an insurance in another company, in



order to prevent fraudulent activities. If no insurance is found the new insurance is made and that information becomes available to all the companies in the network. The information is available very quickly preventing the client to have time to leave the company and run to another company to make another insurance of the same car (See Figure 20).

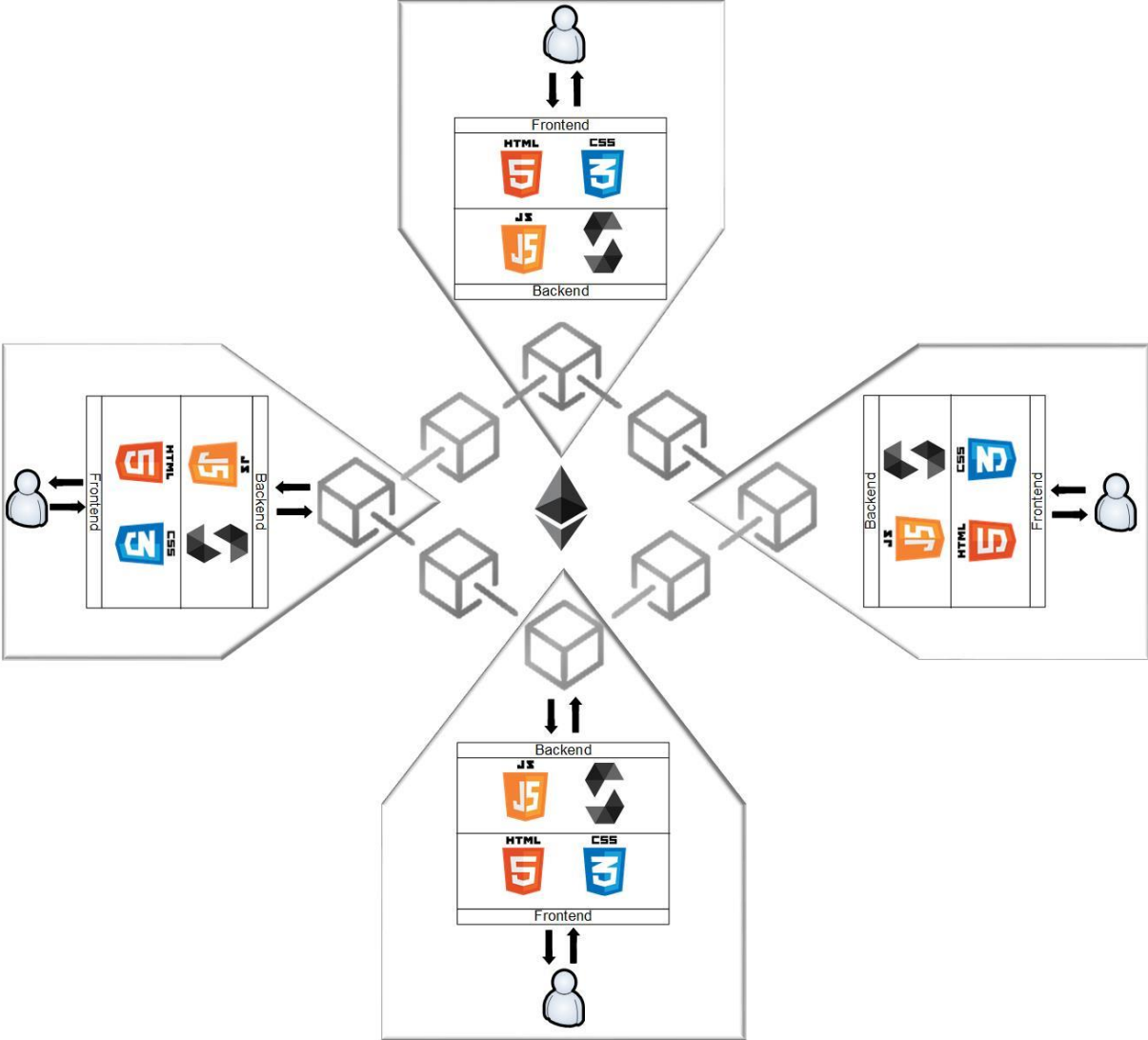


Figure 21 - Blockchain solution architecture for Insurance Companies

In this architecture (Figure 21), every Insurance company has a frontend and a backend present in their system. The frontend is where the user interacts with the DApp (Decentralized Application). The interface is quite simple and intuitive making use only of two programming languages (HTML and CSS). As for the backend, this is where all the logic of process to the Blockchain is going to be made. Only two languages are used here as well (JavaScript and Solidity).

Every system represents a node of the Blockchain. When an employee creates a new insurance, it first must pass all the criteria present in the Smart Contract so by then the transaction can be submitted to the Blockchain and sent to everyone.

### 5.3 Tools

In the following pages, a brief description of the tools used to implement the solution is presented.

#### - Solidity



*Figure 22 - Solidity logo*

As the Blockchain used for the system is Ethereum, it's necessary to use its own language, Solidity (Figure 22). Solidity is going to be used to code all the business logic into the Smart Contracts so the verifications upon creating an insurance can be checked (Ethereum, 2018). Ethereum was the first decentralized app platform and because of this is the Blockchain platform that has the most developers building real-world applications on top of it. Besides this, since the creation of Ethereum many developers have been developing multiple tools (Truffle, Infura, Web3.js) to help other developers create their DApps easily. So, for all the reasons, availability and easy access to information, tools and notorious success of the technology, the Ethereum was chosen for the development of this DApp.

#### - Node.js



*Figure 23 - node.js logo*

Node.js (Figure 23) is an open source and cross-platform runtime environment for executing JavaScript code outside of a browser. Node.js is used to build back-end services, also called APIs. These are the services that power client applications like a web app running inside of a web browser or a mobile app running on a mobile device. These client apps are simply what the user sees and interacts with

they're just the surface they need to talk to some services sitting on the server or in the cloud to store data, send emails or push notifications, kick off workflows, etc.

Node.js is ideal for building highly scalable data intensive and real-time back-end services that power applications.

Why choose node.js instead of other tools?

- Node.js is easy to get started with and can be used for prototyping and agile development;
- Can also be used for superfast and highly scalable services. It's used in production by large companies such as PayPal, Uber, Netflix, Walmart and so on. In fact, at PayPal, they rebuilt one of their Java and Spring based applications using node.js and they found that the node.js app was built twice as fast with fewer people, in 33% fewer lines of code and 40% fewer files and, more importantly the double the number of requests served per second while decreasing the average response time by 35%;
- Node.js has the largest ecosystem of open source libraries available to everyone.

For the development of this system, it's going to be used the Node Package Manager from node.js. Node Package Manager (npm) is a package manager for the JavaScript programming language and is the default package manager for the JavaScript runtime environment Node.js. It consists of a command line client, also called npm, and an online database of public and paid-for private packages, called the npm registry. The registry is accessed via the client, and the available packages can be browsed and searched via the npm website. The package manager and the registry are managed by npm, Inc (Node.js, 2016).

## **- Truffle Framework**



*Figure 24 - Truffle framework logo*

Truffle (Figure 24) is a development environment, testing framework and asset pipeline for Ethereum. It is one of the most widely used IDEs in the Ethereum community. Developers can use it to

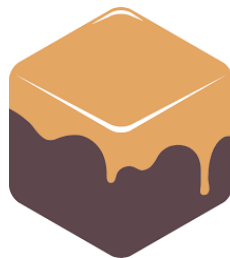
build and deploy DApps for testing purposes with many features that make it more attractive to users with a Web 3.0 dev background.

It has built-in Smart Contract compilation, linking and deployment, so it takes care of managing the contract artefacts. Includes support for custom deployments, library linking and complex Ethereum applications. Whether it is compiling contracts or running unit tests, Truffle includes clever optimizations to ensure that only compiles what the developer must, and tests run as quickly as possible. When used along with Ganache (See below), it can develop DApps quickly and get real code deployed, fast. Truffle has a console which allows access to all deployed contracts for a quick test of the system functioning.

Inside this framework there is also Mocha which is a feature-rich JavaScript test framework running on Node.js and in the browser, making asynchronous testing simple. Mocha tests run serially, allowing for flexible and accurate reporting, while mapping uncaught exceptions to the correct test cases.

The point of Truffle in this work is to help the author organize his DApp development asset and not have to worry about manually setting up a test environment (Truffle, 2018).

## - Ganache



*Figure 25 - Ganache logo*

Ganache (Figure 25) is a personal Blockchain for Ethereum development that can be used to deploy contracts, develop your applications, and run tests. It is available as both a desktop application as well as a command-line tool (formerly known as the TestRPC). Ganache is available for Windows, Mac, and Linux. This tool is going to be our Blockchain (Truffle, 2018).

## - MetaMask



*Figure 26 - MetaMask logo*

MetaMask (Figure 26) is a browser plugin which allows users to make transactions to Ethereum or other networks through browsers, eliminating the need for dedicated user interfaces for Ethereum or other networks.

For example, a user bought a book from a store. He gets the payment details for that deal, but he wants to pay with Ether. To do this, he would need to write the transaction into the Ethereum network, through an Ethereum node, and then broadcast it across the network. The store would then look at the Blockchain and check if the Ether was correctly transferred to its account.

Regular web browsers do not know how to connect to an Ethereum node and read and write to the Blockchain, so it would be necessary a special browser like Mist. This is where MetaMask helps, it makes regular browsers being capable of writing such transactions into the Blockchain, by injecting a JavaScript library called web3.js into the name space of each page the browser loads. Browsers are then capable with functions that can make requests write and reads to Blockchain. It also allows users to specify to which Ethereum node these requests are sent to.

On this system, MetaMask is going to be used to facilitate the process of confirming and inserting transactions into the Ganache Ethereum (Kumavis & Finlay, 2018).

## - Sublime



*Figure 27 - Sublime logo*

To write the code of the Smart Contracts the text editor used is Sublime (Figure 27). This text editor has a Solidity package to color the author's code, so he can have a quick understanding of what he's writing (Sublime, 2018).

## 5.4 Demonstration

In this section, the purpose is to demonstrate the system functioning to handle the cases it was made for: Create an Insurance and submit to the Blockchain; see all the insurances created; stop insurances from being created when a car already has one; and end insurances when the contract ends, or the client wants to.

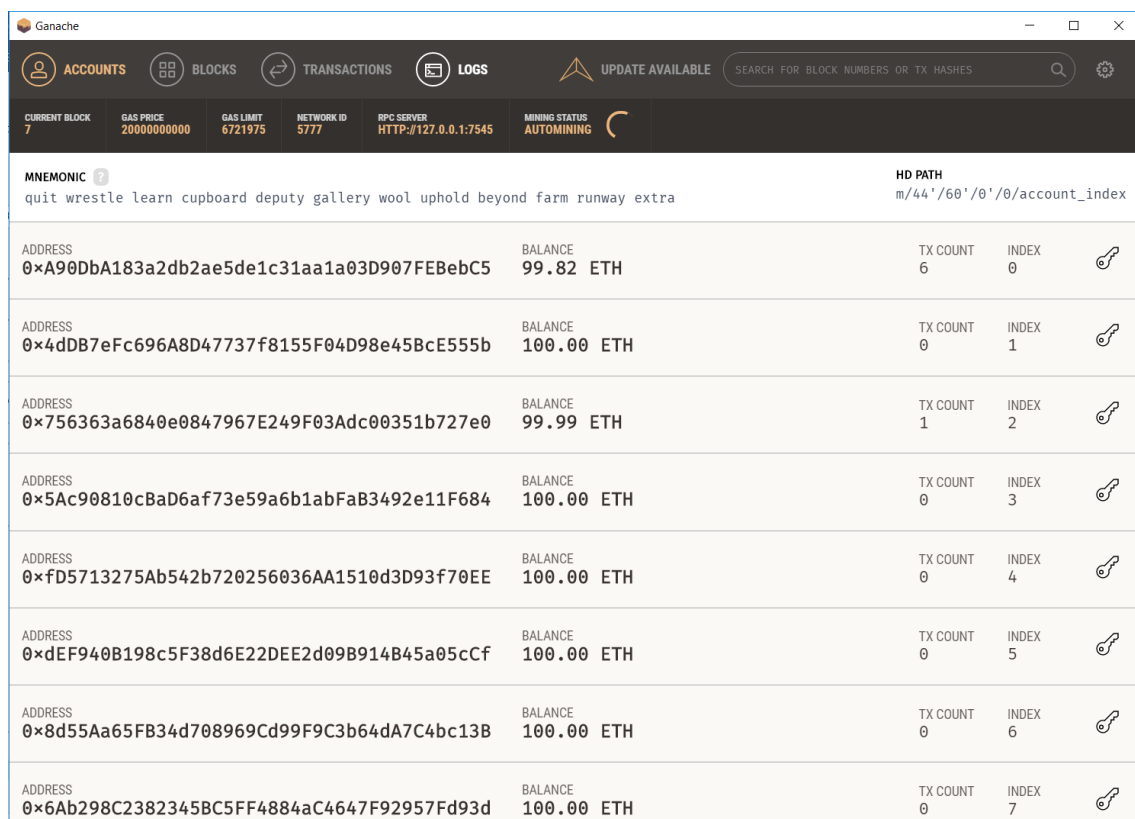


Figure 28 - Ganache interface

In Figure 28, the Ganache app is shown. This app which was described in the tools section, is an application that setup up an Ethereum based Blockchain. In this Blockchain there is 10 accounts/wallets with 100 ETH each for the user to test the system.

```

1  pragma solidity ^0.4.2;
2
3  contract Seguros {
4
5      struct Insurance {
6          uint idInsurance;
7          string idCar;
8          string idPersonCard;
9          uint initialDate;
10         uint endDate;
11         address addrCreator;
12     }
13
14     struct Claim {
15         uint idClaim;
16         string idCar;
17         string idPersonCard;
18         uint date;
19     }
20
21     mapping(uint => Insurance) public insurances;
22     mapping(uint => Claim) public claims;
23
24     uint public insurancesCount;
25     uint public claimsCount;
26
27     event State(string idCar, string idPersonCard, uint date, string description);
28
29     constructor() public {
30     }
31
32     function addInsurance (string _idCar, string _idPersonCard) public {
33
34         bool canCreateInsurance = canCreate(_idCar);
35         require(canCreateInsurance == true, "Car already has an insurance");
36
37         insurancesCount ++;
38         insurances[insurancesCount] = Insurance(insurancesCount, _idCar, _idPersonCard, now, 0, msg.sender);
39         emit State(_idCar, _idPersonCard, now, "Insurance creation");
40     }
41
42     function addClaim (string _idCar, string _idPersonCard) public {
43         bool cCreateClaim = canCreate(_idCar);
44         require(cCreateClaim == false, "Car dont have insurance");
45
46         claimsCount++;
47         Claim(claimsCount, _idCar, _idPersonCard, now);
48         emit State(_idCar, _idPersonCard, now, "Claim");
49     }
50
51     function canCreate(string _idCar) public constant returns (bool) {
52
53         bool canCreateIn = false;
54         for(uint number = 0; number <= insurancesCount; number++) {
55             Insurance storage insurance = insurances[number];
56             if(keccak256(abi.encodePacked(insurance.idCar)) == keccak256(abi.encodePacked(_idCar))) {
57                 if(insurance.endDate == 0) {
58                     canCreateIn = false;
59                 } else {
60                     canCreateIn = true;
61                 }
62             } else {
63                 canCreateIn = true;
64             }
65         }
66         return canCreateIn;
67     }
68
69     function endInsurance(uint _id) public {
70
71         Insurance storage i = insurances[_id];
72         require(0 == i.endDate);
73         require(msg.sender == i.addrCreator);
74         i.endDate = now;
75         emit State(i.idCar, i.idPersonCard, now, "Insurance Ended");
76     }
77 }
78 }

```

Figure 29 - Smart Contract used in the system

For this example, only one Smart Contract called “Seguros” is used (See Figure 29). In this contract, two structs are defined, Insurance and Claims, where all the data related to each will be stored. There is also a mapping for the insurances and is basically a distributed hash table that provide one-move lookups and writes to massive address space. The address space is exclusive to this contract. The keys will be

unsigned integer corresponding to the id of the insurance upon creation, so each key will be corresponding to one insurance.

This contract also has one event called State. As Blockchain is a list of blocks which are fundamentally lists of transactions. Each transaction has an attached receipt which contains zero or more log entries. Log entries represent the result of events having fired from a Smart Contract. In Solidity, to define an event, is used the keyword event. This event will allow to get all the claims and insurances registered to a car (Hitchens, 2017).

The Smart Contract then has 4 functions. “AddInsurance” is used for creating an insurance. For an insurance to be created, the car which will be insured is checked in the Blockchain to see if it has one and this is made by the function “canCreate”. If that condition is met and an insurance is found, the Smart Contracts blocks the creation and throws an error. Otherwise, the creation continues, and the insurance is inserted into the Blockchain with all details given. An event corresponding to this creation is also logged.

To create a claim, the function used is “addClaim”. This process follows the same principles as the previous where a condition needs to be met, however with a small difference. Instead of checking if a car has an insurance, with claims a car needs to have an insurance to create a claim. So, the same function (canCreate) to check the condition is used but the evaluation of the result is different. After finding the insurance of the vehicle, the claim is created and logged.

The last function is “endInsurance “, where two conditions need to be met, the insurance needs to be active and the company, who is trying to end it, needs to be the one that made it.



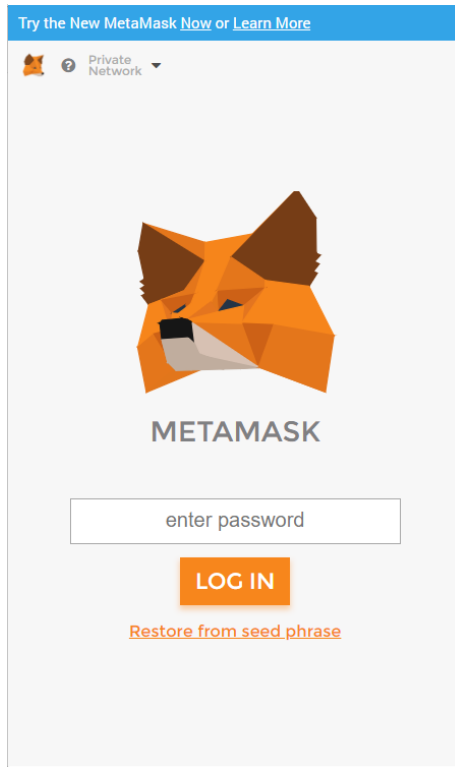


Figure 30 - MetaMask interface

To access MetaMask a password is required. This password is set when initializing it for the first time, so to have access to a wallet it is necessary to know the password (Figure 30).

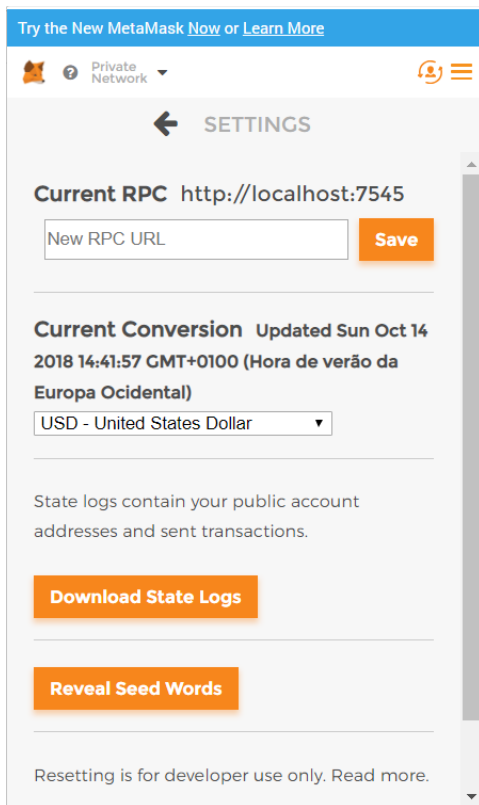


Figure 31 - MetaMask connecting to the right network

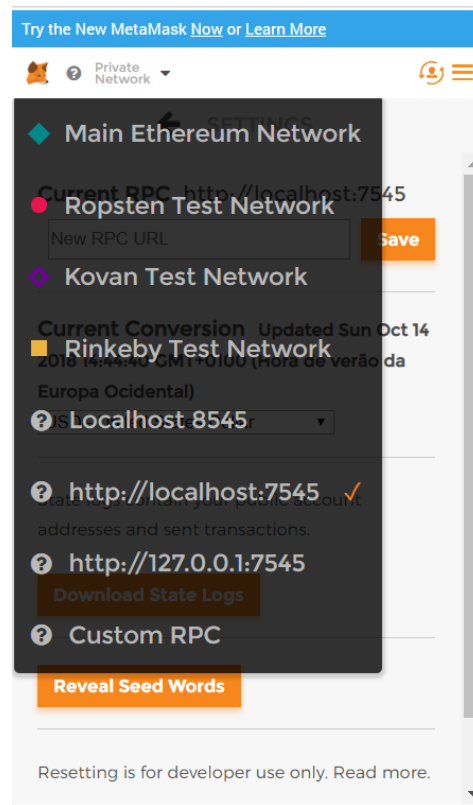


Figure 32 - MetaMask choosing the right network

One of the functionalities of MetaMask is to be able to connect to multiple networks (See Figure 31). So, to be able to connect to the insurance network, it is necessary to insert the network's URL (See Figure 32). In this case, URL inserted is the localhost with the port provided by ganache where the Blockchain is.

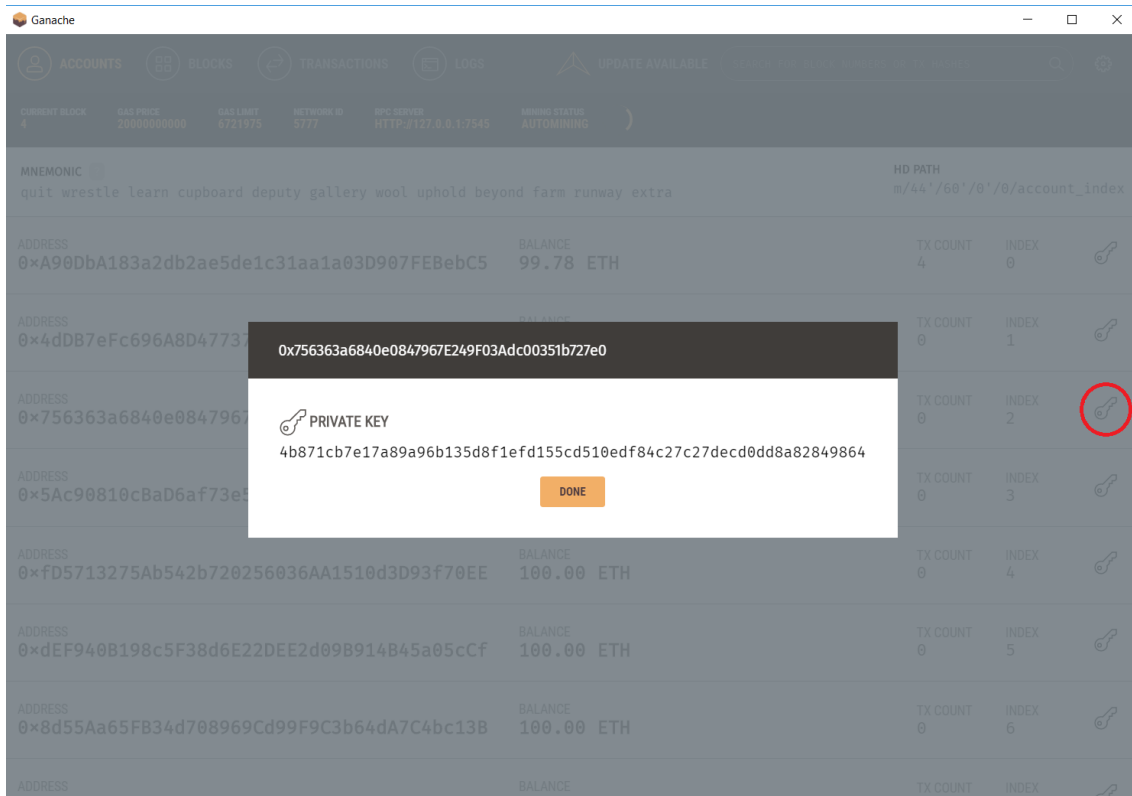


Figure 33 - Private key of an account

After connecting successfully to the network, we need to connect to a certain wallet. The point is, that every insurance company can access to one wallet, so the insurances insert by them can be linked to them. In this case, the third account is picked and to use it with MetaMask it is necessary to insert its private key provided in ganache (See Figure 33).

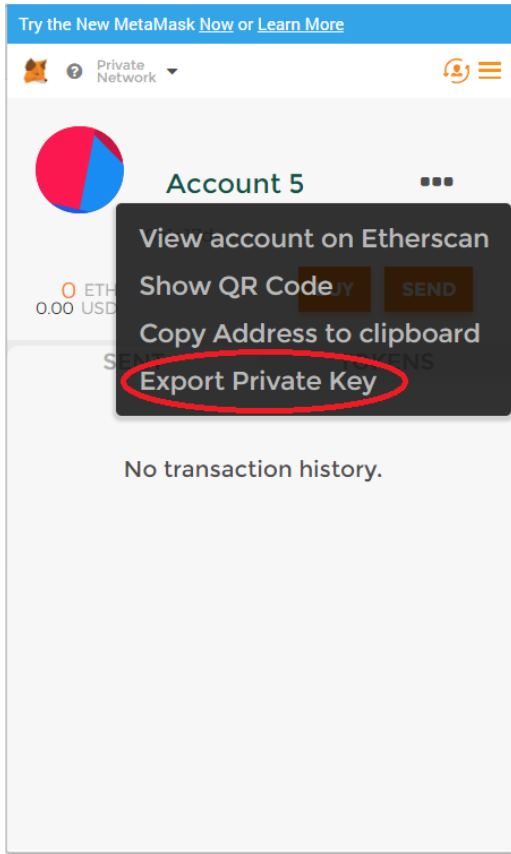


Figure 34 - MetaMask exporting private key for creating account

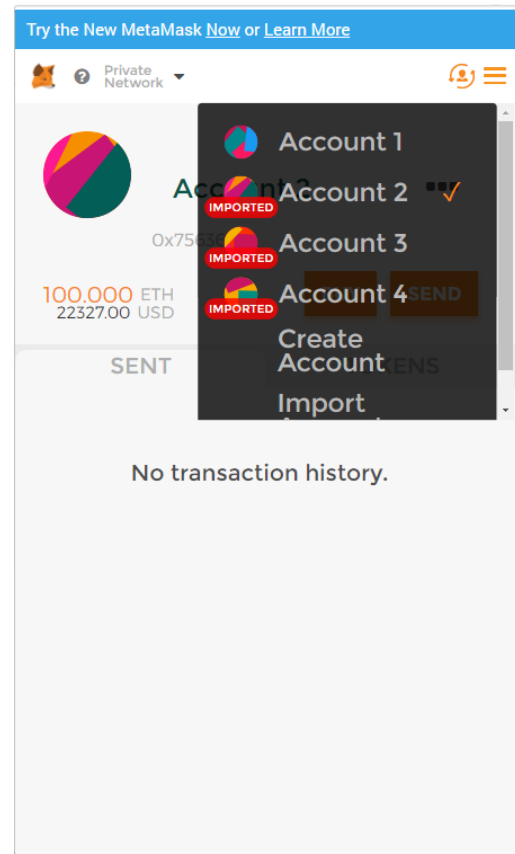


Figure 35 - MetaMask choosing right account

After acquiring the private key from ganache for a certain wallet, the key is inserted on ganache to create an account to start using that wallet (See Figure 34). With the private key, now is possible to use the corresponding wallet, for that is only necessary to choose the right wallet (See Figure 35).

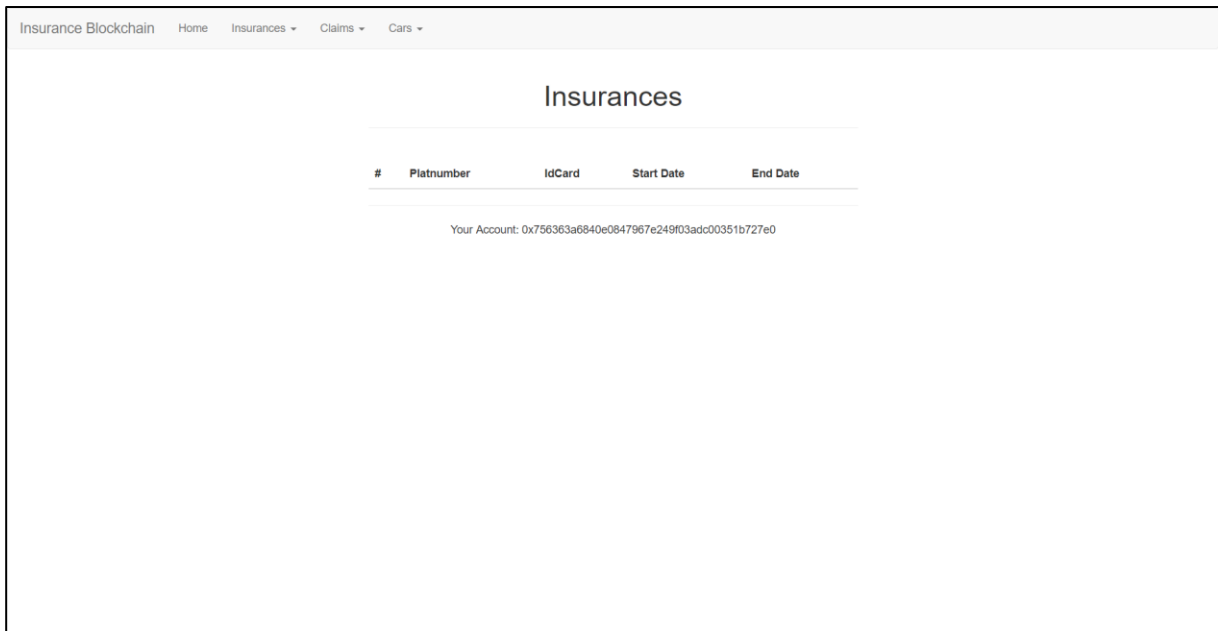


Figure 36 - Blockchain solution interface

This is the index of our web app (See Figure 36). Each Insurance company has its own account, and all can see all the insurances present in the Blockchain. In this case, we're using an account with address "0x756363a6840e0847967e249f03adc00351b727e0" and there is only one insurance created. Using the tools bar in the top of the page, is possible to move around in the web app.

## Create Insurance

**Client idcard**

**Car platnumber**

 -  - 

**Submit**

Figure 37 - Insurance creation form

After pressing in “Create insurance”, it opens a page for doing that task (See Figure 37). For the creation of the insurance its only necessary two fields, client “idcard” and car “platnumber”. As the point of this system is to protect the double creation of insurances leading to the double dipping problem, the client’s id card and the car’s “platnumber” is enough for identifying a person or a car, so additional information is irrelevant. Plus, lesser irrelevant information submitted into the Blockchain is better as it is a way for saving storage space.

**Create Insurance**

---

**Client idcard**

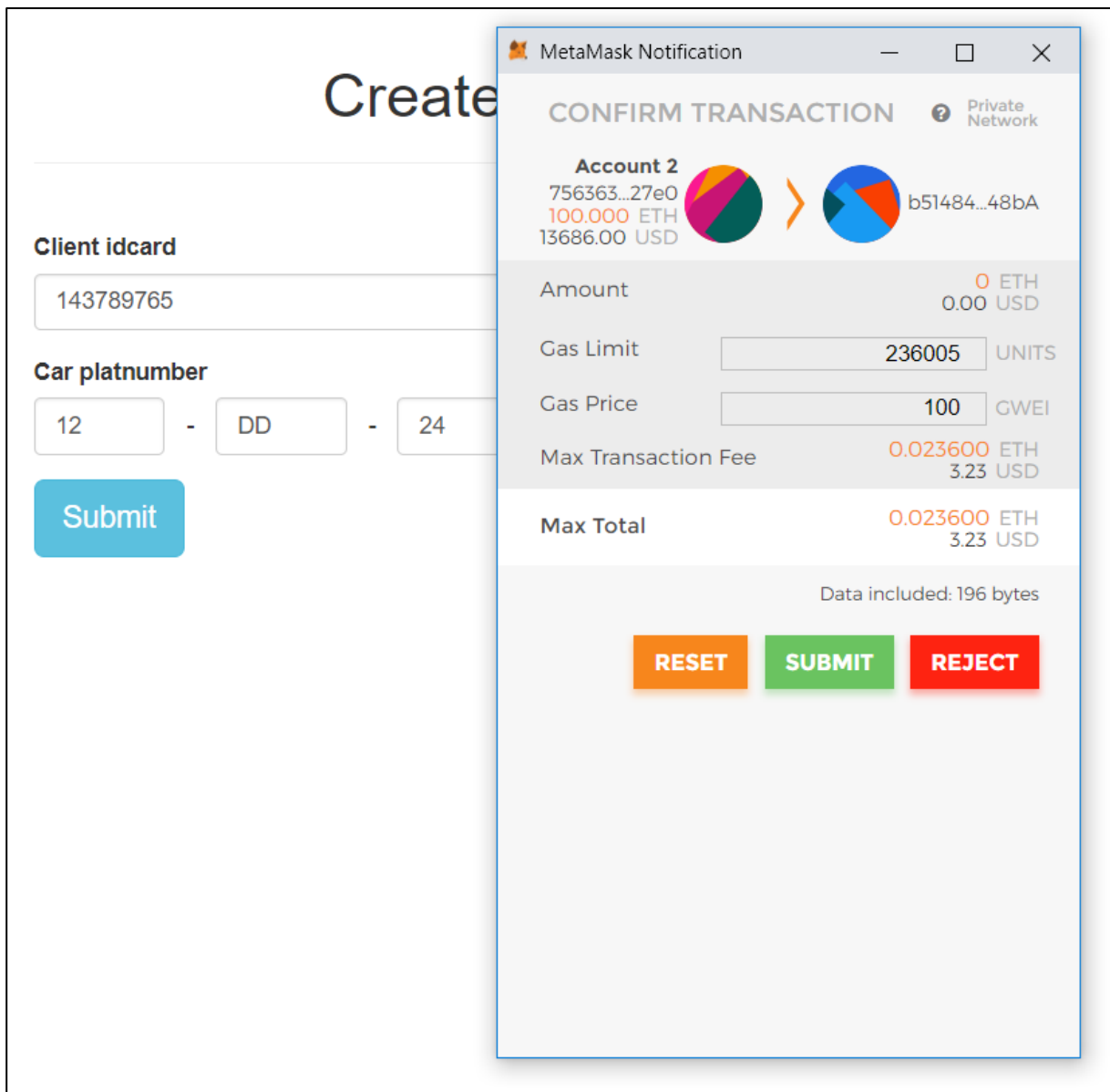
**Car platnumber**

 -  - 

**Submit**

Figure 38 - Insurance creation example

After asking for the information to the user, it is written in the form (See Figure 38). The fields have validation for the length of the id and the “platnumber”, so mistaken information can’t be submitted.



*Figure 39 - MetaMask user transaction confirmation after form submitted*

After pressing the button submit, a pop-up of MetaMask appears (See Figure 39). This pop-up is a confirmation for the transaction it is going to be made and all the transaction's cost Gas and ether. As explained in the chapter 2, for a transaction to be validated, miners as to mine it and for that they get paid by the transaction creator.

In Ethereum, Gas is a measurement unit of computational effort that is needed to be paid to the Ethereum Client to commit the transaction to the Blockchain network. The senders of the message/transactions pay this cost. At the very high level, gas is the number of instructions used to execute a transaction in the Ethereum Virtual Machine. In the Ethereum architecture, it ensures that an

appropriate fee is being paid by transactions submitted to the network. By requiring that a transaction pays for each operation it performs, Ethereum ensures that the network doesn't get misused (Jani, 2017).

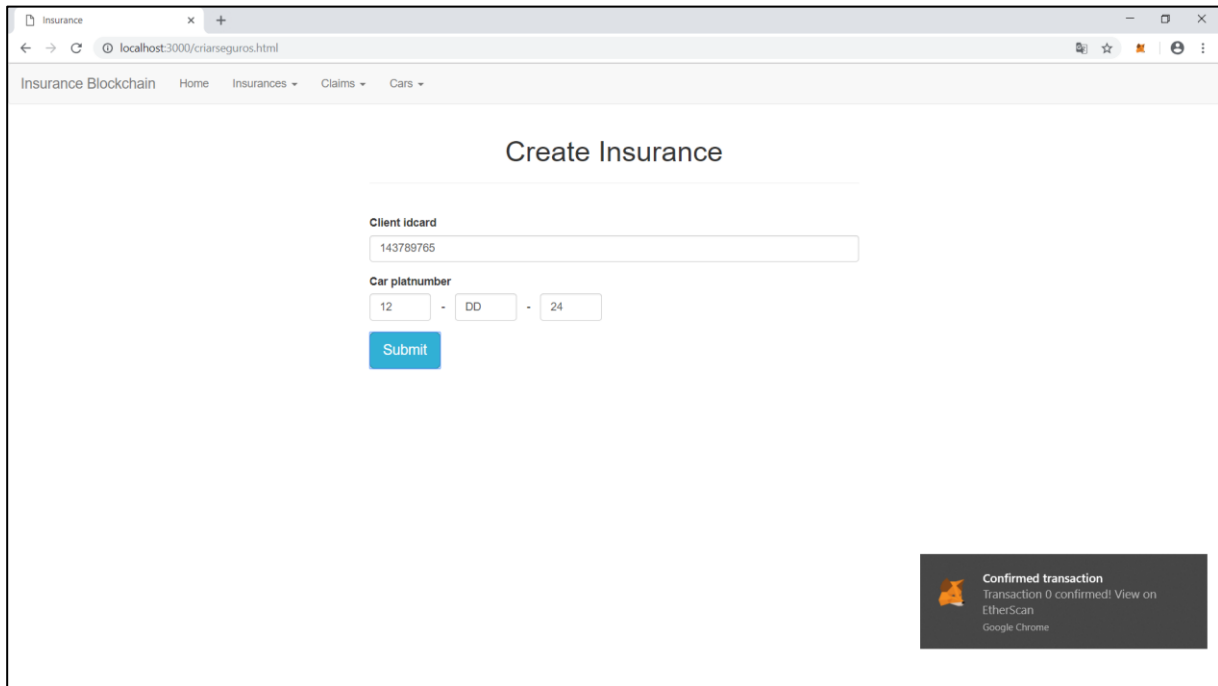


Figure 40 - Ganache transaction confirmation of success

Pressing in the green button “Submit” the process continues and the transaction is submitted into the Blockchain. This transaction fulfills all the criteria present in the Smart Contract and was approved so a pop-up on the bottom left appears confirming it was successfully made (See Figure 40).

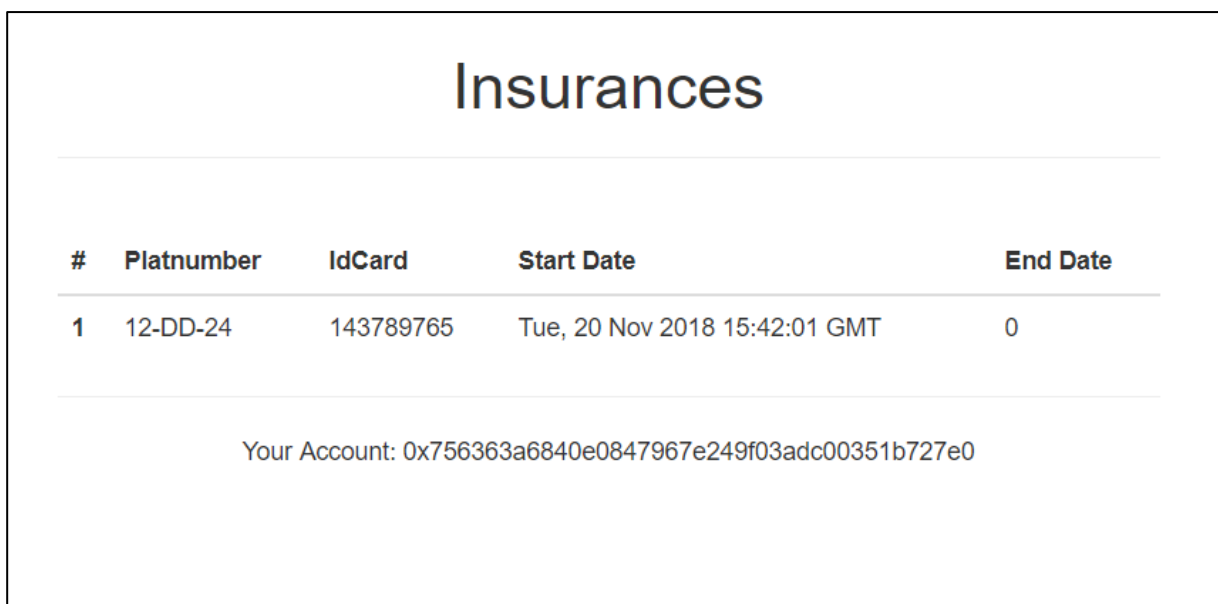


Figure 41 - All the insurances linked to an account of an insurance company

Once submitted, it appears to everyone present in the network. As shown in the Figure 41, there is the new insurance for the car and person inserted. The data stored for each insurance is:

- Platnumber – Unique number for identify a car
- Idcard – Unique number for identify a person
- Start Date – Corresponding to the date an insurance was made
- End Date – Corresponding to the date where an insurance is over. In this case the value is 0 which means the car has an insurance.

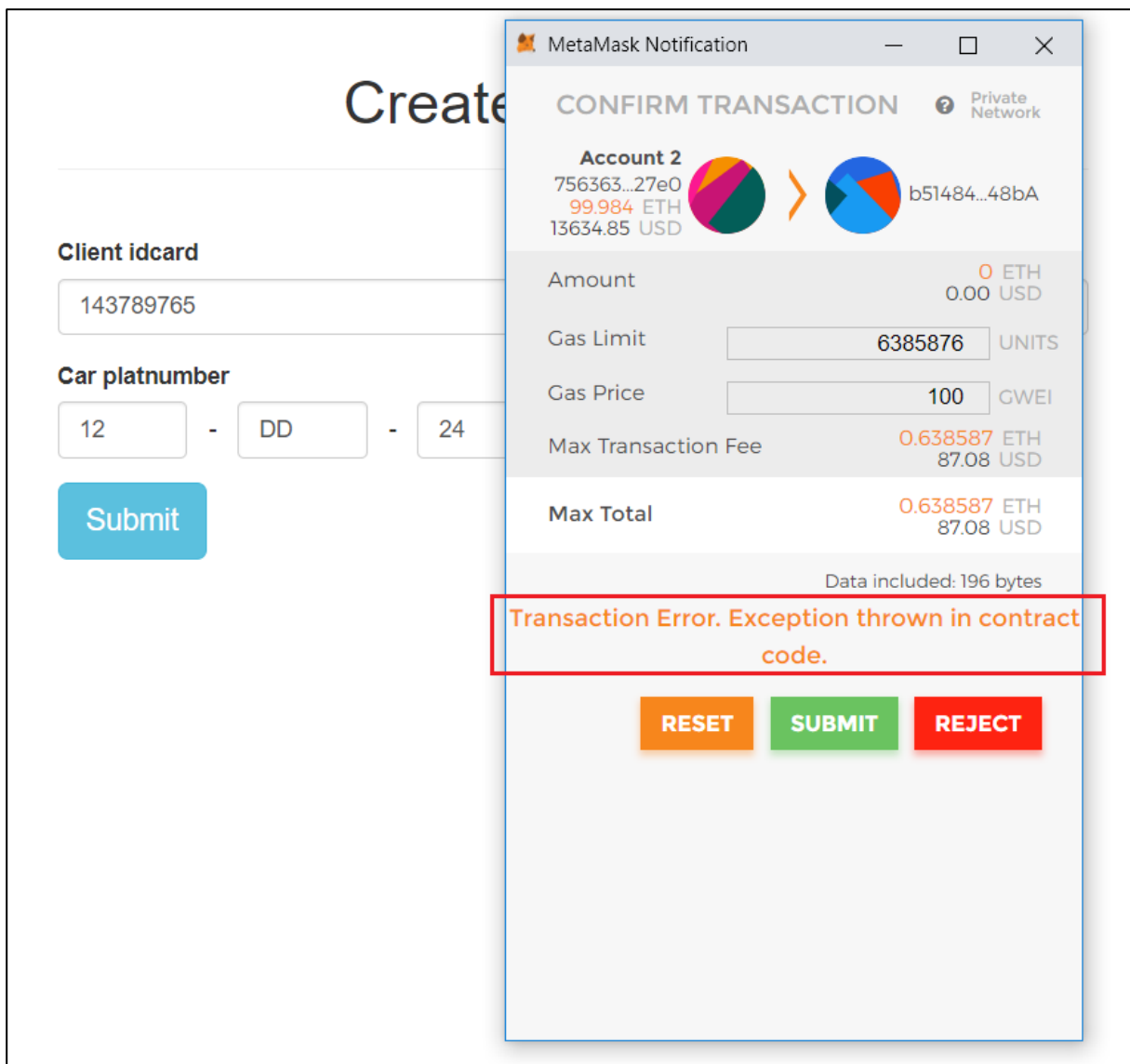


Figure 42 - Error caught by the Smart Contract for not being valid

Going back to the page for create insurances and inserting the same values it will prompt an error. This error is thrown by the Smart Contract when it finds a car which already has an insurance in the system (See Figure 42).



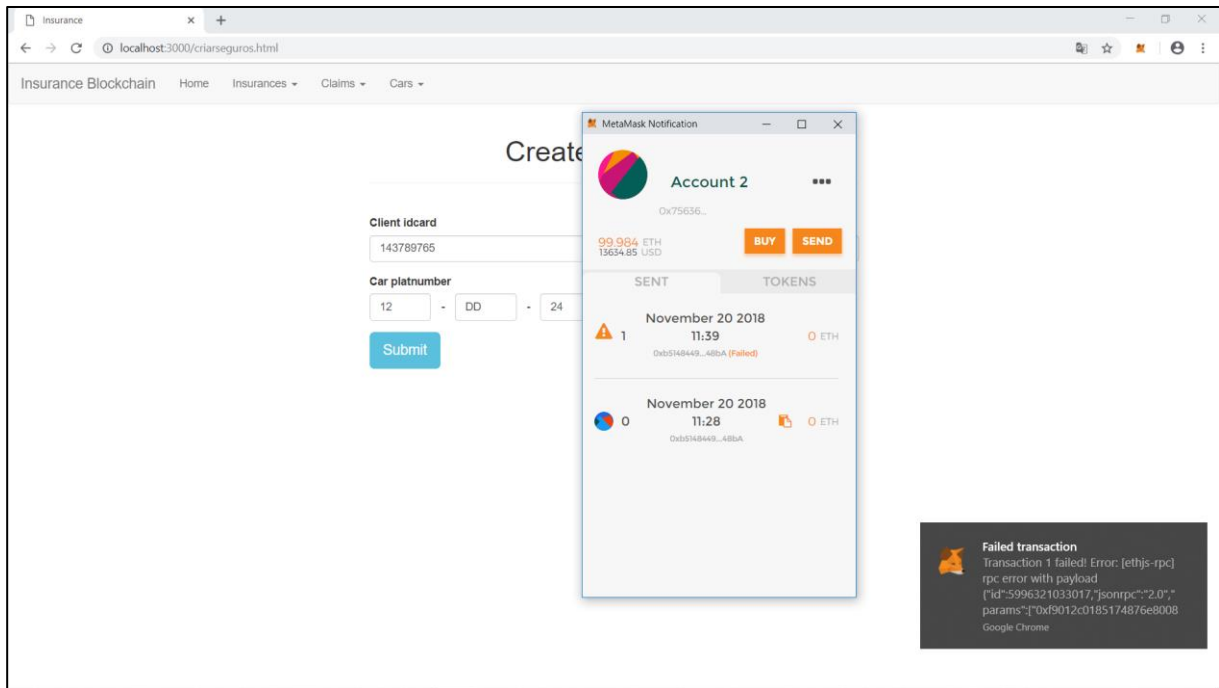


Figure 43 - Error message for failed transaction

As the “platnumber” is the same of the previously insurance created, the transaction will fail because it will be reprovved in the Smart Contract as it won’t fit or comply with all the criteria necessary for the transaction to be validated (See Figure 43).

## Create Claim

---

**Client idcard**

**Car platnumber**

 -  - 

**Description**

Figure 44 - Claim creation form

When a client has an accident, he needs to report what happened to the company. Every accident is also submitted into the Blockchain where the Smart Contract is called to handle claims (See Figure 44). In the Smart Contract, verifications are also made. For example, it is necessary to check if the car has an insurance in the company and if that insurance is active.

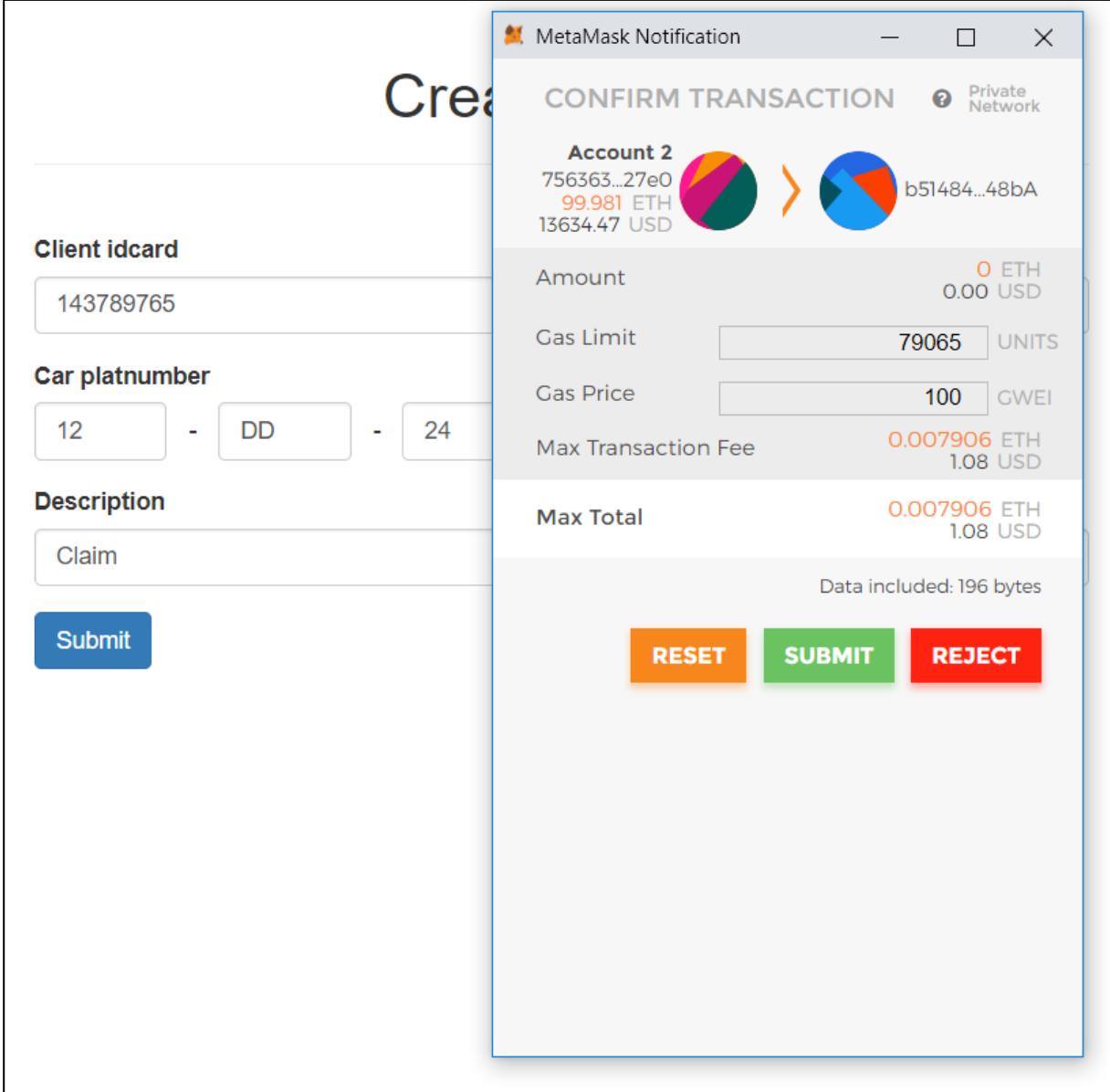


Figure 45 - Claim transaction user confirmation

The report is very simple, it just needs the client's "idcard", car's "platnumber" and a description of the sinister. After this information has been submitted the rules of the previous transactions also applies to this one. A MetaMask's pop up appears to confirm the transaction (See Figure 45).

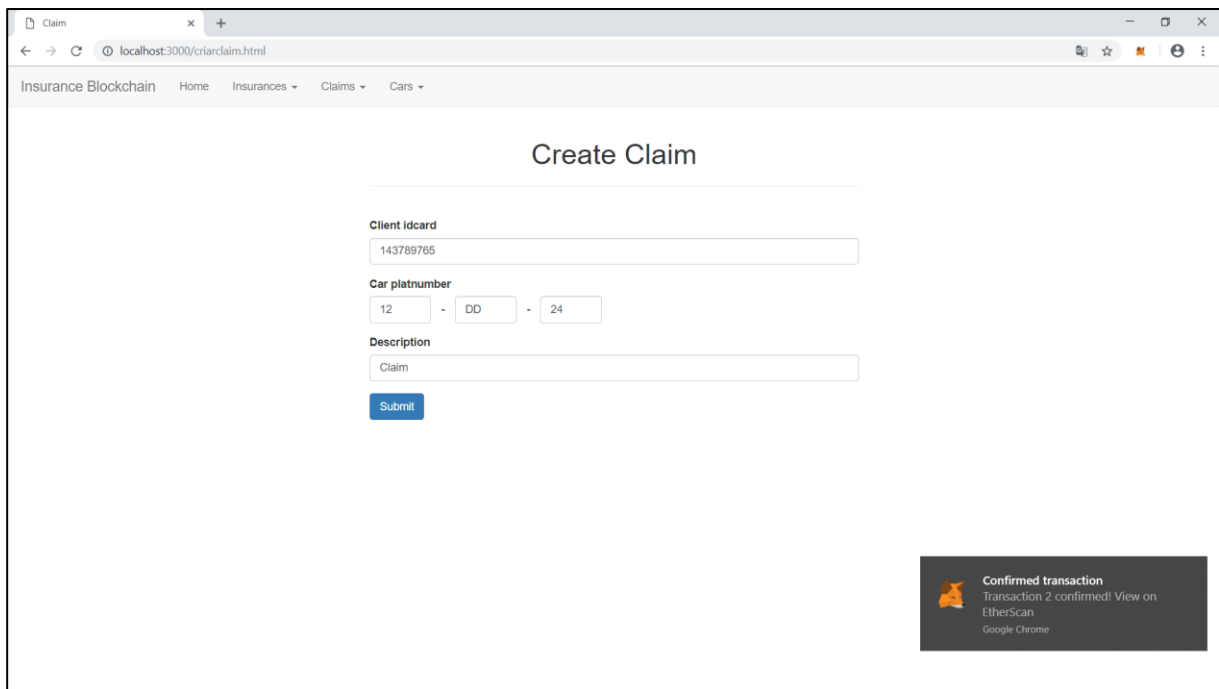


Figure 46 - Transaction confirmation after being submitted

After submitted, the transaction is then mined and added to the Blockchain (See Figure 46). The newly report appears now in the table of the others claims for the company to see.

## Insurance Claims

---

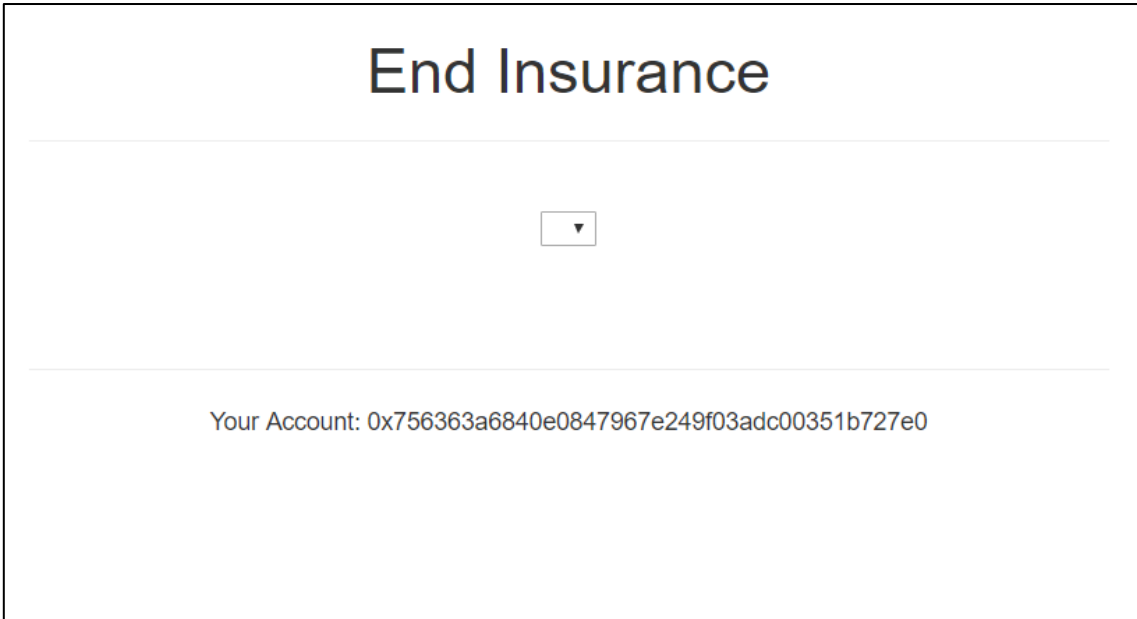
IdCard	Platnumber	Date	Description
12-DD-24	143789765	Tue, 20 Nov 2018 15:43:17 GMT	Claim

---

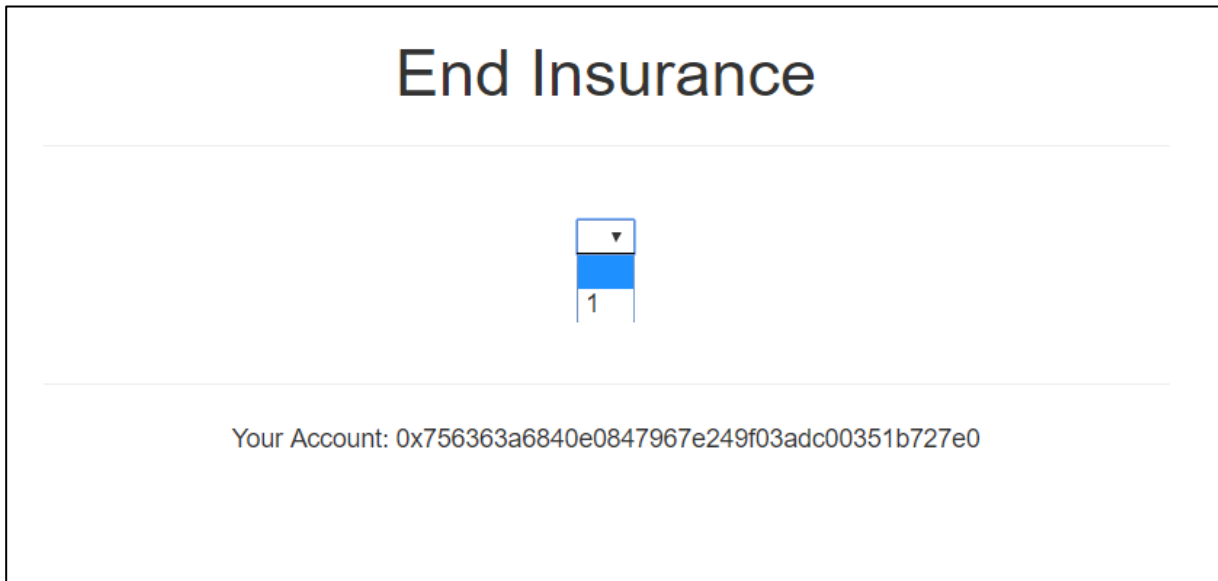
Your Account: 0x756363a6840e0847967e249f03adc00351b727e0

Figure 47 - All claims linked to the wallet of an insurance company

An insurance company can also access all the claims related to vehicles insured by it. In Figure 47, it is possible to see other claims involving other cars and the claim done for testing the claiming creation process.



*Figure 48 - End Insurance interface*



*Figure 49 - Select shows all active insurances*

Every insurance sooner or later ends because of multiple reasons, the owner is unhappy with that insurance and wants to switch or he sold the car and the new owner needs to make a new insurance. In Figure 48 and 49, an insurance can be ended by the insurance company.

# End Insurance

---

1 ▾

idInsurance: 1

idCar: 12-DD-24

idPersonCard: 143789765

Initial Date: Tue, 20 Nov 2018 15:42:01 GMT

End Date: 0

Insurance Company: 0x756363a6840e0847967e249f03adc00351b727e0

Submit

---

Your Account: 0x756363a6840e0847967e249f03adc00351b727e0

*Figure 50 - All data related to the insurance selected appears*

Pressing in the select, it will be shown all the insurance data corresponding to the address of an insurance company. For this case, it is presented the insurance made in this example. After pressing it, all the details corresponding to that insurance is shown for a last check if everything is alright (Figure 50).

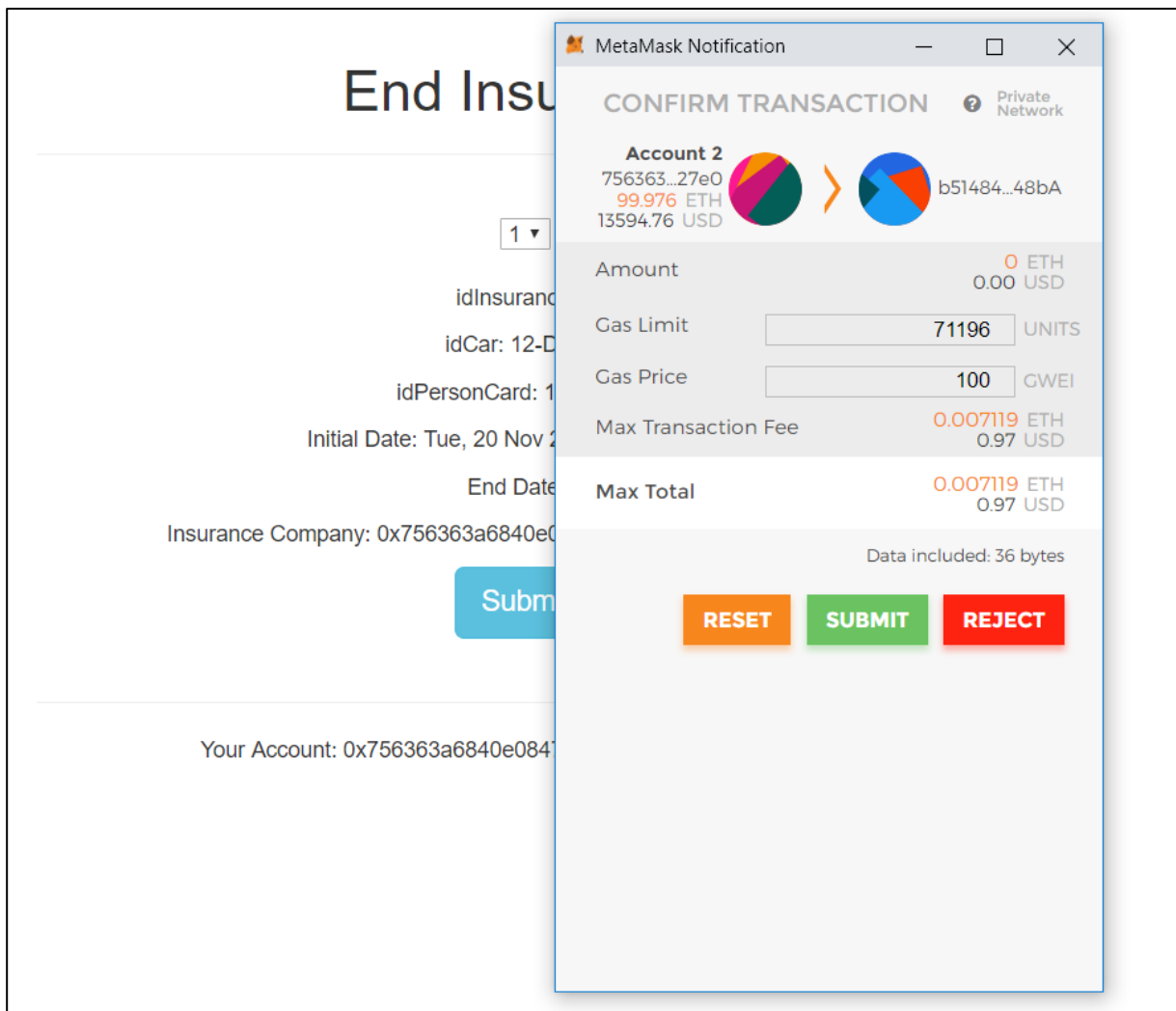


Figure 51 - Confirmation of the transaction end insurance

Pressing in the blue submit, a pop-up for confirming the transaction appears (See Figure 51). The process follows the same steps as a transaction for creating an insurance.

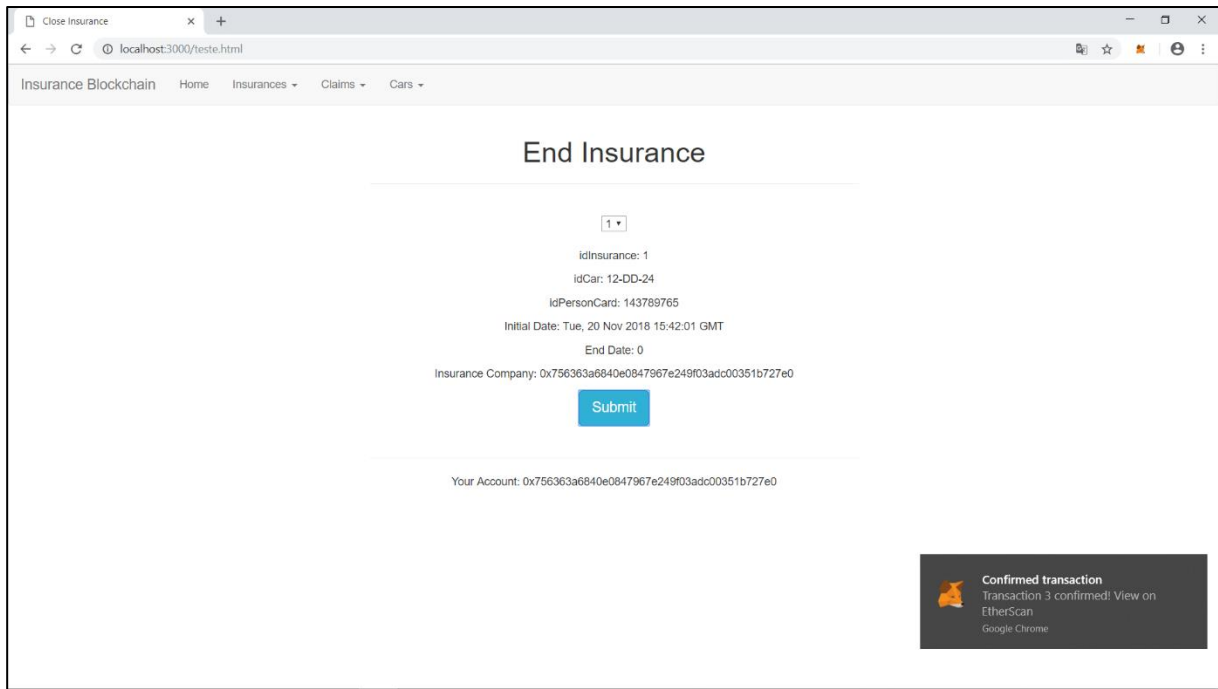


Figure 52 - Confirmation of the insurance submitted into the Blockchain

After submitting the confirmation, an alert is shown confirming the transaction was successfully added to the Blockchain (See Figure 52).

## Insurances

#	Platnumber	IdCard	Start Date	End Date
1	12-DD-24	143789765	Tue, 20 Nov 2018 15:42:01 GMT	Tue, 20 Nov 2018 15:45:52 GMT

Your Account: 0x756363a6840e0847967e249f03adc00351b727e0

Figure 53 - After ending an insurance it gets an end date

In the insurances page, the insurance ended in the example has acquired an end date. This date corresponds to the date when the insurance was ended by the insurance company. So, when an insurance company tries to make a new insurance for the vehicle “WW-31-VT” it will be created because the previously insurance is no longer active.

# Insurances

<input type="text" value="12-DD-24"/>	<input type="button" value="Search"/>		
Platnumber	IdCard	Date	
12-DD-24	143789765	Tue, 20 Nov 2018 15:45:52 GMT	Insurance Ended
12-DD-24	143789765	Tue, 20 Nov 2018 15:43:17 GMT	Claim
12-DD-24	143789765	Tue, 20 Nov 2018 15:42:01 GMT	Insurance creation

Your Account: 0x756363a6840e0847967e249f03adc00351b727e0

*Figure 54 - Car history records*

One of the objectives of this system, is to use Blockchain to record all events a car suffers. So, if an insurance company wants to know all the records about a car, it just needs to search by the plate number and everything appears in a chronological order. In Figure 54, it is possible to see all the transactions we made in this scenario with the car we used.



## 5.5 Conclusion

*“Needless to say, this isn't how companies do business – there's always a human element to establishing a relationship.” – Jason Bloomberg*

The objective of this chapter is to develop a Blockchain based solution that shows all the knowledge acquired. The idealized system acts in the Insurance area and pretends to be a solution to not only give answer to a problem insurance companies face, but also integrate all of them into one Blockchain system. The problem they face it is frauds because sometimes they are very difficult to be detected causing a lot of loss to the organization. One fraud in specific is “Double Dipping” which consists in making an insurance in multiple companies of the same vehicle and later simulating an accident, so the thief can receive money from different companies for the same accident.

To fight this, the suggested system consists on integrating all the insurances companies in a Blockchain network, in other words, every company would be a node of the network. So, when a client goes to a company to create an insurance on his car the company would insert it into the Blockchain and if the client went to other company to create another insurance for the same car when the company tries to insert the insurance into the network the verification made in the Smart Contract would not allowed the insurance to be made because that car would already have an insurance linked to it. As every company, security is a main concern, so this Blockchain network would only let each company see its insurances. Besides this, the system also allows the insurance companies access to car history to see how many insurances it has made and how many accidents it suffered. This is important because upon creating an insurance, the company can access to the history of accidents a person had and adjust the price corresponding to the insurance.



## 6. Conclusion

According to the title of the present dissertation work – Blockchain and Smart Contracts: An Exploratory Analysis – the objectives defined were:

- Review fundamentals and literature of Blockchain and Smart Contracts – Regarding the first objective, as in any research work, it is necessary to know the relevant concepts and become more fluent in the specific research area. This is accomplished through a literature review and by exploring the work of our peers. Since Blockchain is a complex concept, is necessary to invest plenty of time to really understand it. This was a difficult task to accomplish, however, the objective was achieved.

- Study of economical areas with potential for Blockchain solutions – This second objective consists in studying areas where these technologies can be implemented. The most well-known area where Blockchain had more impact, until now, is the financial. However, there are already many areas that are taking advantage of this technology. Besides all the use cases about Blockchain and Smart Contracts, is important to analyze each case and see if it does really make sense the introduction of these technologies. Many new solutions use these technologies only because they are trending, and the essentially same work can be done with technologies already used before.

- Being fluent with a programming language related to Blockchain and Smart Contracts - The language adopted is Solidity which is used by the Blockchain of Ethereum. It is a very intuitive language, however, like every new programming language in the initial phase it is hard to learn but as soon as more time is invested the knowledge increases and the initial difficulties are surpassed. Besides, empiric knowledge acquired during the course about other languages is useful in this phase.

- Development of a Blockchain Solution with support for Smart Contracts - This objective had also some difficulties about the choice of the area to apply the solution. Even though the technology is very promising and with a lot of potentialities to many different areas, it was difficult to find a problem simultaneously interesting and challenging which stands out from the rest. However, this difficulty was overcome, and the solution developed is innovative and relevant to solve the problem identified in the insurance sector. The problem is about frauds, more specifically double dipping, that consists in creating two insurances for the same car in different insurance companies and the report an accident in two companies and gain in double the money for the same accident. For these reasons, Blockchain and Smart Contracts technologies might help improve the Insurance area. A Blockchain solution where insurance

companies can insert the policies of their clients without worrying with frauds related to the creation of multiple insurances for the same car.

Given the complexity and importance of a master thesis, it is necessary to adopt an approach which helps in the execution of the research work. The methodology chosen to assist the author was DSR (Design Science and Research).

In this work, all the relevant concepts related to Blockchain and Smart Contract were defined: Blockchain, Smart Contracts, Distributed Ledger, Consensus Mechanism and Blockchain Types. After all the concepts have been defined, a more detailed explanation of how the Blockchain works was shown. The way how the data is encrypted, how the validation of the blocks is made, how the chain maintains its logic and why the Blockchain can't have its data corrupted were discussed.

Regarding the areas with potential for introducing Blockchain technology, four areas were chosen from a survey answered by key people in the industry:

Finance industry and the current system relies on a high degree of trust in an environment where financial institutions record individuals' accounts in a centralized manner and banks' reserves are stored by a central bank. Blockchain could impact this area by re-thinking how the "central bank" acts by using its decentralization and promise of removing the "middle men". Also, as already seen with bitcoins, a new kind of money transactions have appeared that can potentially threaten the conventional one. This new transaction has advantage of being able to perform even cross-boarders ignoring high transaction fees.

Digital identity consists on using uniquely data to describe a person or a thing and information about the subject's relationships to other entities. In our days, Internet has a great need for Blockchain based identity authentication. There are some ways of identity a person in the physical world using, Social Security numbers, drivers' licenses or passports however when it comes to online authentication of personal identities or identify digital entities there is no such thing. Blockchain technology may be the solution because of the elimination of a central and trusted central authority.

In Property Title, Blockchain also has potential. A use case can be a shared database where people who want to rent a house can see every offer. Once a client gets interested in a house, he can get information about the history of it and even contact with the owner. If both reach an agreement, Smart

Contracts can handle all the money transaction and all the bureaucracy inherent to this kind of agreement. This integration could improve not only monetarily but also the speed of the process.

Communication industry can also benefit with the integration of Blockchain and Smart Contracts. With the growth of social media, many opportunities came with it. Social media give people and organizations major exposure to the others. Some people started to gain fame through it exclusively by posting content made by them and viewers liking it and following it. These content creators are called influencers and because of all the fan base they have organizations look at them as a way of marketing for their business. Marvin combines this new “business” and combines it with Blockchain. There are two main roles in the platform, influencers and marketers. In Marvin’s platform, anyone can be an influencer, even the smaller ones, so everyone can get paid according to the traffic and media mentions they generate. Marketers use Marvin to reach the influencers and paid them to help promote their products. A person with a group of followers recommending a product can have a major impact instead of a TV star advertising.

Besides business areas, four of the most trending technologies areas where Blockchain will have more impact are also studied:

IoT can be combined with Blockchain to help preserve and maintain logic in all the data collected. One example of it is the traditional fish business, where there is a lot of problems, i.e., fishing practices are illegal, unregulated or unreported; after being caught the fish get label no corresponding to him (Seafood fraud) and when is stored the process may be in improper conditions. All this way of business management has impacts in the consumer’s final product quality and there is no way for the consumer to know, creating a lack of vendor and consumer trust. To prevent these problems, combining IoT, Blockchain and Smart Contracts could be the solution. Recording the trip of all sea-food since when it was fished from the sea until it gets to the final consumer. IoT sensors can be attached to any object entrusted to someone else for transport, with trackable ownership, possession, and telemetry parameters such as location, temperature, humidity, motion, shock and tilt. The final buyer can access a complete record of information and trust that the information is accurate and complete.

Another technology is Big Data. In bigger organizations, databases can go up to Petabytes, so companies need to guarantee that all the data centers are synchronized in real time and all the data is authentic Blockchain combined with Big Data can bring many benefits to Financial Industry, in the field of analytics. As data stored in Blockchain has the promised of being secured relatively to forging and

corruption, this data can be used for analysis purposes. Also, the data is structured making it good for analysis. For example, a Blockchain network that allows financial institutions check all the transactions happening in real time. Once a transaction happens, the bank could analyze it in real time and see if there was any fraud involved. As for the current system, where the fraud prevention is made by analyzing all the records of the fraud.

The last technology is AI. The main goals of a Blockchain is a constant update of all the data stored and this data is very secure because of the cryptography used by it. While AI tries to achieve the best decision, it can use the data stored from the Blockchain and get better results with highly reliable information. As explained before, Proof of Work (PoW) consists in multiple miners trying to solve algorithms to find the best solution and once found the block is sent to all nodes. AI works in the same idea, to take a decision the machine analyses every possible solution until it finds the best under a certain condition. This process requires a lot of computational power and if the decision is very complex it could take some time. Combining AI with Blockchain, all the nodes present in the network could participate in the task of taking a decision. This way, the process would be divided to everyone and it would take less time.

After this, a description of the business area where is going to be introduced Blockchain's mechanisms. The area chosen is Insurances more precisely car insurances. Insurances has a long history, in China, each boat transported only a small part of merchandise from each merchant. In case of sinking or robbery only a part of the goods of each one was lost. This ancient way of prevention consists in the fragmentation or distribution of the risk to minimize the losses if something happens. Nowadays, it has evolved a lot however it still has a lot of bureaucracy and exhaustive processes where technologies can help to improve them. Besides this, as old as Insurances, Frauds have been around since its creation. People are always trying ways to gain easy money from insurance companies by simulating losses.

Finally, the demonstration case is presented, in which an alternative Blockchain based system is suggested for fighting the double dipping fraud was presented. As explained before, double dipping consists of making two insurances on two different companies and when an accident happens receive money from the two companies. To fight this, the suggested system consists on integrating all the insurances companies in a Blockchain network, in other words, every company would be a node of the network. So, when a client goes to a company to create an insurance on his car the company would insert it into the Blockchain and if the client went to other company to create another insurance for the same

car when the company tries to insert the insurance into the network the verification made in the Smart Contract would not allowed the insurance to be made because that car would already have an insurance linked to it. As every company, security is a main concern, so this Blockchain network would only let each company see its insurances. Besides this, the system also allows the insurance companies access to car history to see how many insurances it has made and how many accidents it suffered. This is important because upon creating an insurance, the company can access to the history of accidents a person had and adjust the price corresponding to the insurance.

For future work, it is suggested to apply the Blockchain and Smart Contracts to other types of insurance. One of the insurances that can also benefit from it is personal objects (computers, cell phones, suitcases) because frauds is not only present in cars.





## References

- Arasev, V. (2018, January). POA Network Whitepaper. Retrieved from <https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper>
- Auto-ID Labs*. (1999). Retrieved January 27, 2018, from <https://autoidlabs.org/>
- Back, A., Corallo, M., Dashjr, L., Friedenback, M., Maxwell, G., Miller, A., . . . Wuille, P. (2014, October 22). Enabling Blockchain Innovations with Pegged Sidechains. Retrieved December 10, 2017, from <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>
- Benos, E., Garratt, R., & Gurrola-Perez, P. (2017, August). The economics of distributed ledger technology for securities settlement. *Bank of England*.
- Brennan, C., & Lunn, W. (2016, August 3). Blockchain: the trust disrupter. *Credit Suisse Securities (Europe) Ltd.: London, UK*.
- Brennan, C., Zelnick, B., Yates, M., & Lunn, W. (2018, January 11). Blockchain 2.0. *Credit Suisse*.
- Cameron, K. S., & Quinn, R. E. (2011). *Diagnosing and changing organizational culture: Based on the competing values framework*. John Wiley & Son.
- Cant, B., Khadikar, A., Ruitter, A., Bronebak, J. B., Coumaros, J., Buvat, J., & Gupta, A. (2016). Smart Contracts in Financial Services: Getting from Hype to Reality. *Capgemini Consulting*.
- Christidi, K., & Devetsikiotis, M. (2016, May 10). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*.
- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2015, October 16). Blockchain Technology: Beyond Bitcoin. *Sutardja Center for Entrepreneurship & Technology Technical Report, UC Berkeley*.
- Diffie, B. W., & Winius, G. D. (1977). *Foundations of the Portuguese Empire*. University of Minnesota Press.
- Doebeli, G., Fisher, R., Gapp, R., & Sanzogni, L. (2011). Using BPM governance to align systems and practice. *Business Process Management Journal*.

- Dumas, M., Rosa, M. L., Mendling, J., & Reijers, H. A. (2013). *Fundamentals of Business Process Management*. Springer-Verlag Berlin Heidelberg.
- Ethereum. (2018, October 12). Solidity Documentation. *Ethereum*. Retrieved from <https://media.readthedocs.org/pdf/solidity/develop/solidity.pdf>
- Fintechnews. (2017, June 14). *Blockchain Use Cases in Financial Services*. Retrieved from <http://fintechnews.sg/9981/blockchain/blockchain-use-cases-financial-services/>
- Frei, C., Wilkinson, A., Trepte, F., & Hatop, O. (2017). The Developing Role of Blockchain. *World Energy Council*.
- George, G., Haas, M. R., & Pentland, A. (2014, April 4). Big Data and Management. *Academy of Management Journal*. Retrieved from [http://ink.library.smu.edu.sg/lkcsb\\_research/462](http://ink.library.smu.edu.sg/lkcsb_research/462)
- Greenspan, G. (2015). MultiChain Private Blockchain – White Paper. *MultiChain*. Retrieved from <http://www.multichain.com/download/MultiChain-White-Paper.pdf>
- Guo, Y., & Liang, C. (2016, December 9). Blockchain application and outlook in the banking industry. *Financial Innovation 2*.
- Hitchens, R. (2017, February 20). *Solidity CRUD- Part 1*. (Medium) Retrieved from <https://medium.com/@robhitchens/solidity-crud-part-1-824ffa69509a>
- Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia computer science*.
- Hussain, F., Ferworn, & Zahid, J. I. (2017, November). Integrating Internet of Things and Blockchain: Use Cases. *IEEE Internet Initiative*.
- Hyperledger. (2016). *Seafood Case Study in Supply Chain*. (Hyperledger) Retrieved from <https://sawtooth.hyperledger.org/examples/seafood.html>
- Hyperledger Fabric. (2017). A Blockchain Platform for the Enterprise. Retrieved from <https://hyperledger-fabric.readthedocs.io/>
- i2S. (2012). A História Universal do Seguro.
- Instituto de Seguros de Portugal. (2006, October 24). Sistema de Colocação de Contratos de Seguro Obrigatório de Responsabilidade Civil Automóvel Recusados. *Norma Regulamentar N.º 9/2006-R*.

- Jani, S. (2017, December 8). An Overview of Ethereum & Its Comparison with Bitcoin. *International Journal of Scientific & Engineering Research*.
- Jentsch, C. (2017, January 2). *Public vs Private chain*. Retrieved from <https://blog.slock.it/public-vs-private-chain-7b7ca45044f>
- Johnston, B. (2008). Identifying, Avoiding & Curing The Double Dip. *TenPoint Insurance Solutions*.
- Karp, N. (2015, July 10). Blockchain Technology: The Ultimate Disruption in the Financial System. *US Economic Watch*.
- Khatwani, S. (2017, July 12). *What Are Private Blockchains & How Are They Different From Public Blockchains?* Retrieved from <https://coinsutra.com/private-blockchain-public-blockchain/>
- Kumavis, & Finlay, D. (2018). *MetaMask Browser Extension*. (MetaMask) Retrieved 2018, from <https://github.com/MetaMask/metamask-extension>
- Kuyoro, S., Osisanwo, F., & Akinsowon, O. (2015, March). Internet of Things (IoT): An Overview. *3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM'2015)*.
- Larimer, D. (2014, April 3). Delegated Proof-of-Stake (DPOS). Retrieved from <https://steemit.com/bitshares/@testz/bitshares-history-delegated-proof-of-stake-dpos>
- Larimer, D. (2017, May). DPOS Consensus Algorithm - The Missing White Paper. Retrieved from <https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper>
- Liu, D., & Camp, L. J. (2006). Proof of Work can Work. *WEIS*.
- Ma, H.-D. (2011, November 28). Internet of Things: Objectives and Scientific Challenges. *Journal of Computer Science and technology*.
- Mark, J. J. (2011, April 28). *Roman Empire*. Retrieved from [https://www.ancient.eu/Roman\\_Empire/](https://www.ancient.eu/Roman_Empire/)
- Mavin. (2018, February 12). A reward-based influencer marketing ecosystem on blockchain. Retrieved from <https://icorating.com/upload/whitepaper/WMCICuYN0bRZFzf7Jj4YbkzxCpKFIW1H1JApjRlt.pdf>
- McWaters, R. J. (2016, August). A Blueprint for Digital Identity—The Role of Financial Institutions in Building Digital Identity. *World Economic Forum*.

- Medland, D. (2015, June 28). *Cost Of Regulation 'Top Concern' For Financial Services*. (Forbes) Retrieved from <https://www.forbes.com/sites/dinamedland/2015/06/28/cost-of-regulation-top-concern-for-financial-services/#a97f0a1e133d>
- Milani, F., García-Bánuelos, L., & Dumas, M. (2016, October). Blockchain and Business Process Improvement. *BPTrends newsletter*.
- Ministério das Finanças. (1998, April 17). Decreto-Lei n.º 94-B/98. Retrieved from <https://dre.pt/application/conteudo/474478>
- Ministério das Finanças e da Administração Pública. (2007, Agosto 21). Decreto-Lei n.º 291/2007. Retrieved from [https://dre.pt/web/guest/legislacao-consolidada/-/lc/72930793/201705032047/exportPdf/normal/1/cacheLevelPage?\\_LegislacaoConsolidada\\_WAR\\_drefrontofficeportlet\\_rp=indice](https://dre.pt/web/guest/legislacao-consolidada/-/lc/72930793/201705032047/exportPdf/normal/1/cacheLevelPage?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice)
- Ministério das Finanças e da Administração Pública. (2008, April 16). Decreto-Lei n.º 72/2008. Retrieved from [https://dre.pt/web/guest/legislacao-consolidada/-/lc/105326879/201704171114/exportPdf/normal/1/cacheLevelPage?\\_LegislacaoConsolidada\\_WAR\\_drefrontofficeportlet\\_rp=indice](https://dre.pt/web/guest/legislacao-consolidada/-/lc/105326879/201704171114/exportPdf/normal/1/cacheLevelPage?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice)
- Morrison, E. D., Ghose, A. K., Dam, H. K., Hinge, K. G., & Hoesch-Klohe, K. (2011, December). Strategic Alignment of Business Processes. *International Conference on Service-Oriented Computing*.
- Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Nakamoto, S. (2009, August 30). *Blockchain Original Source Code*. Retrieved from <https://github.com/bitcoin/bitcoin/tree/4405b78d6059e536c36974088a8ed4d9f0f29898>
- Negro, M. D., & Tao, M. (2013, February 22). *Historical Echoes: Cash or Credit? Payments and Finance in Ancient Rome*. (Liberty Street Economics) Retrieved from <http://libertystreeteconomics.newyorkfed.org/2013/02/historical-echoes-cash-or-credit-payments-and-finance-in-ancient-rome.html#.V1GF-PkrLcs>
- Node.js. (2016). About Node.js. Retrieved from <https://nodejs.org/en/about/>
- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017, March 20). Blockchain. *Business & Information Systems Engineering*.

- Nolan, S. (2014, July 4). Staged Collisions: Separating Accidents from Fraud. *Insurance Institute of Ireland*. Retrieved from [https://www.iii.ie/upload/publications/docs/No.7\\_StagedCollisions.pdf](https://www.iii.ie/upload/publications/docs/No.7_StagedCollisions.pdf)
- O'Connell, J. (2016, June 20). *What Are the Use Cases for Private Blockchains? The Experts Weigh In*. Retrieved from Bitcoin Magazine: <https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/>
- Oluwatosin, H. S. (2014, February). Client-Server Model. *IOSR Journal of Computer Engineering*.
- Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*.
- Peterson, J., Krug, J., Zoltu, M., Williams, A. K., & Alexander, S. (2018, July 12). Augur: a Decentralized Oracle and Prediction Market Platform.
- Pilkington, M. (2015, September 18). Blockchain Technology: Principles and Applications. *Research Handbook on Digital Transformations*.
- Pinna, A., & Ruttenberg, W. (2016, April 26). Distributed ledger technologies in securities post-trading - Revolution or evolution? *ECB Occasional Paper No. 172*.
- Plattfaut, R., Niehaves, B., Pöppelbuß, J., & Becker, J. (2011, June 10). Development of BPM Capabilities - Is Maturity the Right Path? *Proceedings of the 19th European Conference on Information Systems (ECIS)*.
- PORDATA. (2016, 09 18). *Veículos registados por tipo de veículo*. (PORDATA) Retrieved from <https://www.pordata.pt/Europa/Ve%C3%ADculos+registados+por+tipo+de+ve%C3%ADculo-3070-261052>
- PricewaterhouseCoopers. (2014). Threats to the Financial Services sector. Retrieved from <https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf>
- Publiq. (2017, May). PUBLIQ White Paper. Retrieved from <https://publiq.network/en/white-paper/>
- PwC. (2016, July). Real Estate 2020 Building the future. Retrieved from <https://www.pwc.com/sg/en/real-estate/assets/pwc-real-estate-2020-building-the-future.pdf>
- Raghupathi, W., & Raghupathi, V. (2014, February 7). Big data analytics in healthcare: promise and potential. *Health Information Science and Systems*.

- Rosic, A. (2017). *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*. Retrieved from <https://blockgeeks.com/guides/smart-contracts/>
- Russell, S., & Norvig, P. (2016). *Artificial Intelligence: A Modern Approach*. Pearson Education Limited.
- Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference*.
- Savelyev, A. I. (2017, November 25). Copyright in the Blockchain Era: Promises and Challenges. *Computer Law & Security Review*.
- Seffinga, J., Lyons, L., & Bachmann, A. (2017, February). The Blockchain (R)evolution – The Swiss Perspective White Paper. *Deloitte*.
- Sharma, T. K. (2018, January 30). *Blockchain Solutions for Big Data Challenges*. Retrieved from <https://www.blockchain-council.org/blockchain/blockchain-solutions-for-big-data-challenges/>
- Sharma, T. K. (2018, February 25). *How Can Blockchains Transform Artificial Intelligence?* (Blockchain Council) Retrieved from <https://www.blockchain-council.org/blockchain/how-can-blockchains-transform-artificial-intelligence/>
- Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & Infrastructure (Identity, Data Security). *Massachusetts Institute of Technology-Connection Science*.
- Sillaber, C., & Watti, B. (2017, August 5). Life Cycle of Smart Contracts in Blockchain Ecosystems. *Datenschutz und Datensicherheit-DuD*.
- SITA. (2016). *Travel Identity of the Future*. Retrieved from <https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf>
- Skrumble Network. (2018, February). Decentralized Communication Powered By Blockchain. Retrieved from [http://skrumble.network/wp-content/uploads/2018/02/WhitePaper\\_0207\\_v2-min-1.pdf](http://skrumble.network/wp-content/uploads/2018/02/WhitePaper_0207_v2-min-1.pdf)
- Smith, W. (1875). *A 19th-Century Classical Encyclopaedia*. Retrieved from [http://penelope.uchicago.edu/Thayer/E/Roman/Texts/secondary/SMIGRA\\*/Argentarii.html](http://penelope.uchicago.edu/Thayer/E/Roman/Texts/secondary/SMIGRA*/Argentarii.html))A 19th-Century Classical Encyclopaedia
- Sublime. (2018). *Documentation - Sublime text*. (Sublime) Retrieved 2018, from <https://www.sublimetext.com/docs/3/>

- Swan, M. (2015). *Blockchain: Blueprint for a new Economy*. O'Reilly Media, Inc.
- Swiss Re. (2013, August 26). A History of Insurance. Retrieved June 16, 2018, from [http://www.swissre.com/library/archive/A\\_History\\_of\\_Insurance.html](http://www.swissre.com/library/archive/A_History_of_Insurance.html)
- Swiss Re. (2014, Março 24). A History of Insurance in China. Retrieved June 14, 2018, from [http://www.swissre.com/library/archive/A\\_History\\_of\\_Insurance\\_in\\_China.html](http://www.swissre.com/library/archive/A_History_of_Insurance_in_China.html)
- Szabo, N. (1997). The Idea of Smart Contracts. *Nick Szabo's Papers and Concise Tutorials*, 6.
- Tapscott, A., & Tapscott, D. (2017, March 1). How Blockchain Is Changing Finance. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/03/how-blockchain-is-changing-finance>
- Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.
- Tregear, R. (2011, November). Becoming Process Centric. *BPTrends*.
- Truffle. (2018). *Truffle Suite / Ganache*. (Truffle) Retrieved from <https://truffleframework.com/ganache>
- Truffle. (2018). *Truffle Suite Documentation*. (Truffle) Retrieved from <https://truffleframework.com/docs/truffle/overview>
- Valenta, M., & Sandner, P. (2017, June). Comparison of Ethereum, Hyperledger Fabric and Corda. *FSBC Working Paper*.
- Vasin, P. (2014). BlackCoin's Proof-of-Stake Protocol v2. Retrieved from <https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf>
- Vom Brocke, J., & Rosemann, M. (2010). *Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture 2*. Springer-Verlag Berlin Heidelberg.
- Walport, M. G. C. S. A. (2016, January 19). Distributed Ledger Technology: beyond blockchain. *UK Government Office for Science*. Retrieved from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf)
- Whitaker, J. E. (2013, May 14). The state and challenges of insurance fraud. Retrieved July 20, 2018, from <http://www.triglav.hr/wps/wcm/connect/84ced421-5490-4580-b8a9->

8c0fb14a48c7/The-state-and-challenges-of-insurance-fraud.pdf?MOD=AJPERES&CACHEID=84ced421-5490-4580-b8a9-8c0fb14a48c7

Whitaker, J. E. (2018). *Insurance Fraud Handbook*. Association of Certified Fraud Examiners.

Whyte, G. (2017, May 13). *Public Blockchains vs Consortium Blockchains vs Private Blockchains*. Retrieved from <https://www.linkedin.com/pulse/public-blockchains-vs-consortium-private-gavin-whyte>

Windley, P. J. (2005). *Digital Identity: Unmasking identity management architecture (IMA)*. O'Reilly Media.

Wolfond, G. (2017, October). A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review* 7.10.

Yap, S. (2015, August 17). *Blockchain technology to be largest financial industry disruptor*. Retrieved June 22, 2018, from <https://www.dealstreetasia.com/stories/blockchain-technology-to-be-largest-financial-industry-disruptor-bbva-10530/>



## **Annex A – Cientific Publication: IoT applications using Blockchain and Smart Contracts**

**Authors:** Rui Roriz; José Luis Mota Pereira

**Conference:** DSIC18: The 2018 International Conference on Digital Science

**Link:** [https://link.springer.com/chapter/10.1007/978-3-030-02351-5\\_48](https://link.springer.com/chapter/10.1007/978-3-030-02351-5_48)

**Abstract:** Blockchain is a relatively new technology, initially created for the Bitcoin's network to store transaction records happening in it. The system is redundant and distributed, making it difficult for fraudulent transactions. Beyond digital currencies, the Blockchain concept has already demonstrated its potential in the insurance, health, digital identity, and many other areas. In order to deal with specific needs in those areas, a new technology has appeared – Smart Contracts – computational code programmed to meet and enforce certain conditions, like the ones seen in traditional contracts. Taking into account the benefits brought by Blockchain and Smart Contracts, it is important to study their contributions to emerging technological solutions, like IoT (Internet of Things), in which security, connectivity and interoperability are major concerns. This paper aims to describe relevant Blockchain and Smart Contract's concepts, discussing their contribution to support and improve modern IoT solutions.

**Keywords:** Blockchain, Smart Contracts, Internet of Things (IoT).