COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER

Blockchain Technology. What is it, where is used and a practical application

Autor: Nicolás Espinosa de los Monteros Darnaude.

Director: Jorge Herrera de la Cruz

Madrid

Enero de 2019

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. Nicolás Espinosa de los Monteros Darnaude DECLARA ser el titular de los derechos de propiedad intelectual de la obra: Blockchain Technology. What is it, where is used and a practical application, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente).*

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.

d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 14 de Enero de 2019.

ACEPTA

Fdo: Nicolás Espinosa de los Monteros Darnaude

Proyecto realizado por el alumno:

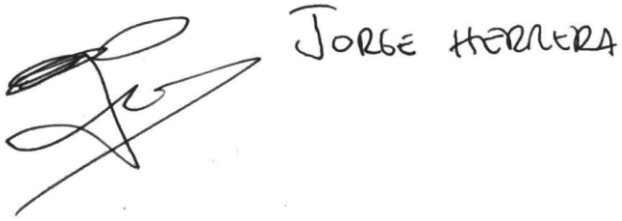
Nicolás Espinosa de los Monteros Darnaude

Fdo:  Fecha: 14/01/2019

Autorizada la entrega del proyecto cuya información no es de carácter confidencial

EL DIRECTOR DEL PROYECTO

Jorge Herrera de la Cruz

Fdo: 

Fecha: 25/01/2019

Vº Bº del Coordinador de Proyectos

Susana Ortiz Marcos

Fdo: Fecha: /01/2019

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER

Blockchain Technology. What is it, where is used and a practical application

Autor: Nicolás Espinosa de los Monteros Darnaude.

Director: Jorge Herrera de la Cruz

Madrid

Enero de 2019

A mi familia,

A Jorge, mi director

A mis amigos,

Al Instituto Católico de Artes e Industrias,

Gracias a todos por aguantarme y apoyarme.

Memory Index

Figure index

Parte I - STUDY

Chapter 1 INTRODUCTION

1. PREVIOUS STUDIES AND SPONSORS

The aim of this research is to show the potential of the new and challenging technology called BlockChain. First of all two coupled questions will be answered in order to clarify this recent methodology:

- What is Blockchain?
- Where is Blockchain used?

There is been polemic surrounding this technology and the fundaments have not been clearly delimited as it is in early stages. After this in depth literature review the limits and possibilities of Blockchain will be set and a practical example of an application of the technology will be explain.

There have been numerous studies made of the impact of the blockchain technology on all sectors of economy. Mainly all investment banks and consulting firms have their researches and publications on the theme as well as lots of public institutions and universities.

The bibliography of this project cites a lot of examples of this trend. Blockchain always deserves an important chapter in any disruptive technology document as everyone coincides that it has come to stay. Throughout this study, investment banking reports will be cited to argument the transformation on economics and consulting firms analyze the potential in business. Institutions centered in Blockchain have appeared to foster its development. Public and governmental institutions are investigating the societal changes it could bring to the table.

Later on, it will be explained that the term was firstly introduced by someone with a pseudonym and has been developed by code communities and institutions. These developments has been made in a practical way focusing on developing tools whether if they are cryptocurrencies, platforms, databases or other digital applications.

Regarding the state of the art, [1] has served as a firm settlement to the knowledge hereby presented. Steve Wozniak (Apple cofounder) or Dan Schulman (CEO of

Paypal) recommend the book for anyone willing to understand the basics of the technology and mainly the future applications and changes this technology will come with it. The book goes into all transformations, cultural and business related that we will face the coming years on where Blockchain will be the cornerstone. In figure 1, to understand how the author sees the magnitude of this technology the first phrase that can be read in the book in the Spanish version is: "Everything is Blockchain".

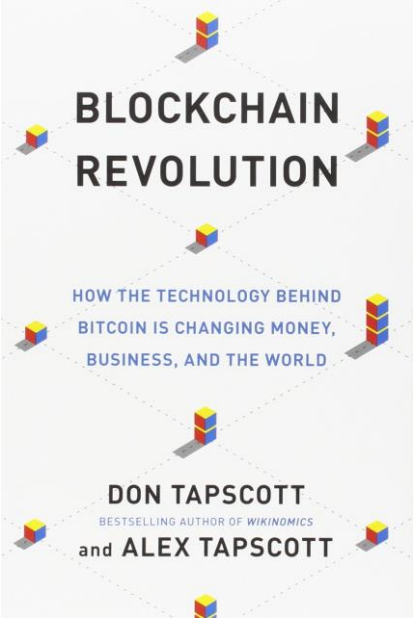


Figure 1. Blockchain Revolution cover [1].

This project will try to offer a different approach than the book, not predicting the different applications or transformations, but having it in mind we will try to answer technically what is Blockchain and where is it used. The study aim to serve as solid foundation to anyone who wants to get its hands on the technical aspects inside the technology as well as providing numerous examples of real life ventures that are leaning on the Blockchain technology.

In a social perspective the United Nations (UN) states that Blockchain has lots of potential for social impact [2]. This has not been the only voice shouting to make of Blockchain a source of prosperity and equality [6]. In figure 2 we have a sample of social projects that based in Blockchain are trying to solve different social problems:

Frame	Project	Idea
Banking	Grassroots Economics	Through community **currencies** people have a way to exchange goods and services and incubate new businesses.
Banking	ChamaPesa	Open network for social **savings** communities to allow people to save and invest.
Access	RightMesh	Allow people without **internet** access to get information by leaping between phones, computers, and other devices until it gets to its destination
Solidarity	Possible.	Enable more people to do **work** that is not valued by the market and increase solidarity

Figure 2. Blockchain social projects sample.

It is interesting the position of Kenya, being one of the fastest growing economies. This country is betting high on Blockchain in its economy. It is also going to receive in its capital the World Blockchain Summit on March 2019 [3]. We also find initiatives like the incubator for Blockchain projects Blockchain for Social Impact [4]. And also in Spain we have found projects that combine blockchain with social needs. Ethichub powers microcredits for small farmers with Blockchain [5].

2. MOTIVATION

Blockchain is a technology that has not arisen from the world of research or academics but from private companies departments of R&D. Despite this fact, it has caught all the mentioned attention and has placed itself among the current edge of technology. However, it is a complex and developing concept that is by the moment highly influenced by its most famous and first application, Bitcoin. This driving force of Blockchain will have its own chapter as it has served as a base to the development.

The origin and its complexity have made it hard to find technical that clearly defines the aspects and limits of the technology. There is plenty of resources to understand how Bitcoin works at a glance. However when more difficult is introduced (SmartContracts and DAPP's will be explained in their subsequent chapter) or other possibilities are taken to the picture it seemed quite diffuse to find the common points and the different technical variables that makes each of them different, unique and meaningful.

The boosters of Blockchain believe it to be the ultimate utility knife of libertarianism in its pure way. The elimination of intermediation and the creation of an independent trust between parties that want to make a transaction felt like the spiritual force that guided to this technology. Even though the anonymity or the security may be the ones responsible for it escalation.

The challenge to breakdown numerous recent technologies and create a conceptual framework, that hopefully will serve the others that find themselves in a starting position. Also aiming to advance and clarify the technical aspects and variations of Blockchain have been great motivations to develop the work. These challenges presented by disruptive and recent technology that as shown in figure 3, that quantifies the Google searches of the concept as a way to measure its relevance, is in the mouth of a lot of people is been another motivation to create this work.

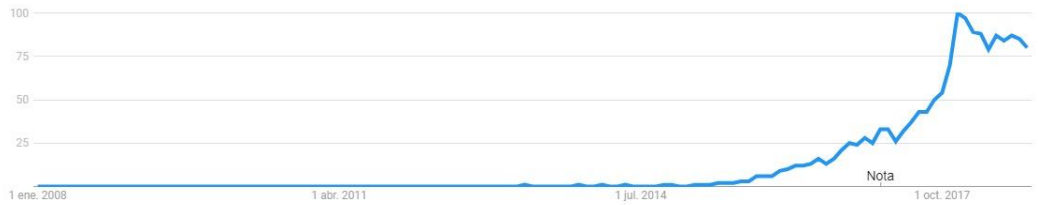


Figure 3. Google searches for Blockchain percentage to its maximum.

As has been commented, making an easier path to the following people with technical knowledge that want to get to technically understand what is behind it to, maybe, create something based on it that will benefit the whole society. This idea of technology development as a force of human progress and wellbeing is the foundation have carried this work forward.

As discussed in [7] the world is better than ever. Attending to the facts proposed in figure 4, world population living in extreme poverty, global child mortality or illiterate world population, it can appear that there is no extreme necessity to propose solutions to social problem. However, this increase in welfare has come in hand with the technological development and this is a boost for contributing to the world to continue this process and minimize inequities.

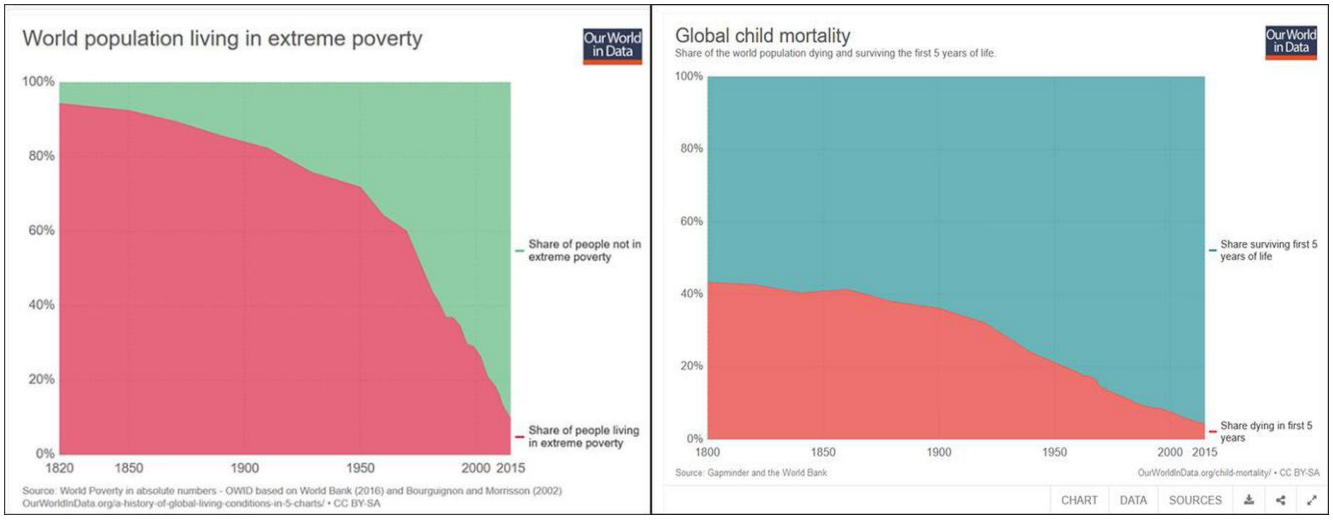


Figure 4. Data showing world's progress [7].

With this motivations, finally the concepts of Blockchain will be applied to a real social problem to show it can be a source of equality and progress to the whole world.

3. GOALS

The goal of this project is to stablish a conceptual framework for technical thinkers to develop Blockchain solutions to existing problems of the world. These main goals are reflected in:

- Defining the technology
- Analyzing the technical concepts of the technology
- Investigate the different possibilities and create a framework to evaluate them.
- Analyzing markets and their interaction with Blockchain.
- Provide an example to Blockchain utilization to solve a social problem.

4. METHODOLOGY

Trying to compile all the knowledge in this field, in this work we show the main clues from a wide range of bibliography. However, due to the non-scientific origin of this technology (as explained before) we also include as sources webs (mainly, but not only, related to coding) and film documentaries giving voice to the main actors of this technology.

The first thing was to gather as much documents as possible. There is vast production of content related to the topic and it was key to select the most suitable ones to include. This work was lasting too much and a course on the topic [Blockchain in the energy sector – Future Learn] helped settle the concepts. With a lot of information in mind, reviews made and other work developed, it was the moment to set the index of what wanted to be done. With this idea in the head finally everything was create a document that will serve technical thinkers get their hands on this technology.

With our goals in mind and the necessity to highlight that Blockchain can be a source of growth and prosperity to developing and third world countries, the focus was put on the absence of legal security in land ownership. In this point, the first thing is to validate the problematic, then to look at the different possibilities and to choose the most suitable one. With a clear route and leveraging the previous work, we set the technical dimensions of the project and the organization.

The realization of this project is been developed over time as shown in figure 5.

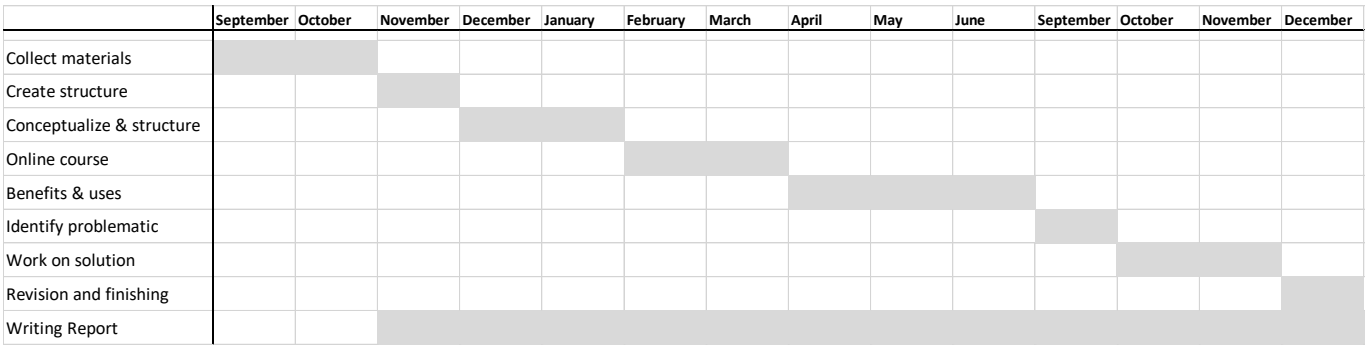


Figure 5. Work calendar timeline.

5. RESOURCES

In order to achieve the previously exposed tasks, the use of certain resources and tools that are explained below have been needed. Also, it has been very important to have access to different sources of technical essays provided by the Universidad Pontificia de Comillas.

i MICROSOFT OFFICE

The Microsoft Office 2013 package, consisting of several types of programs with different functionalities, will be used in this project to cover the needs explained below.

Microsoft Word

This program will be used to carry out the writing of the document that will explain, both the operation of the complete project, and the steps that have been followed to fulfill the objectives explained.

Microsoft Excel

This is a spreadsheet software that will be used during this project. The program has been used for the realization of explanatory.

ii AUTODESK AUTOCAD

AutoCAD is a computer-aided design software (CAD: Computer Aided Design) that allows to draw both in two and three dimensions.

In this case, the student version of Autodesk AutoCAD 2018 has been employee for the design of explanatory graphs in order to facilitate the understanding of the processes that have been developed and the systems that make up the project described in this document.

Chapter 2 WHAT IS BLOCKCHAIN?

1. INTRODUCTION

In this chapter we try to solve the question: What is Blockchain? To do so, we dive in the way of functioning and the history to get a fully understanding of what makes a process worth the Blockchain naming. Also, where does one approach to the technology differ from the other and what are the common elements.

We try to use an integrating perspective of the different modes of operation and to obtain the common minimums and their different ways in order to characterize what belongs to Blockchain technology.

We try to do it without forgetting key elements in its future development as SmartContracts or addressing trendy topics like ICO's but always remaining in the technical side not the controversy.

We firstly have to focus on this method because for example the cryptography or distributed computing are two elements prior to Blockchain that allow numerous different applications, but none of them do not have to be confused with this technology, but there is no Blockchain without both of them.

We could say that Blockchain is like a plate of food that each house or restaurant does in a different way but that we understand when we are named. That is why this chapter will try to identify the minimum ingredients to obtain a blockchain dish and show the different spices and variations to the recipe that can be made, knowing that this can change advance or modify over time, but allowing the reader to generate a conceptual framework to characterize them all.

2. HISTORY

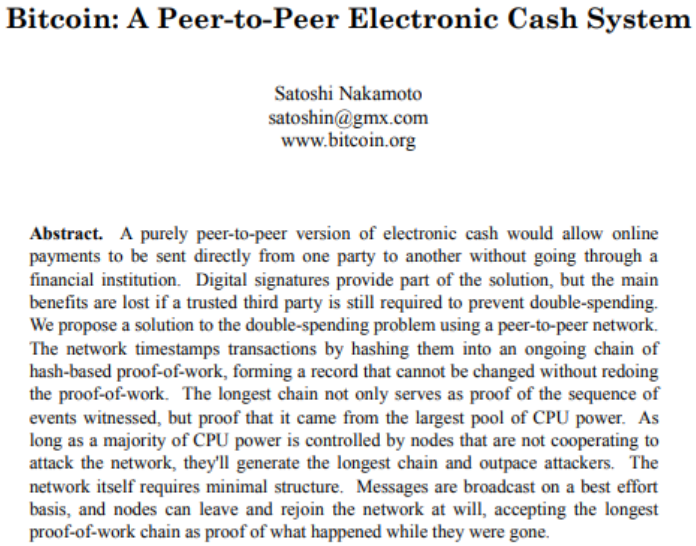
To understand the appearance of Blockchain technologies it is impossible not to start with Bitcoin as it is the cryptocurrency that generated the technology. This part of the study has retrieved knowledge of a documentary [10] and other sources. This documentary is really interesting to understand not just the history of the technological development but also the regulatory one and some other controversial and political aspects that will not have its space on this chapter as they stand out of the scope proposed.

The origin of Blockchain is in the development of cryptocurrencies and its genesis is in the cyberpunk movement in the early 90's that focused on using internet to ensure privacy and liberty. This group of people were hackers agglutinated by the document "A Cypherpunk's Manifesto" of 1992 [11]. As written in the manifesto: *"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."*

The work of this group gave some systems that were really close to happening like the DigiCash initiative started by David Chaum that ended separating from the pure cyberpunk movement. But after all no major initiative trespass to the public opinion. Later, after the financial crisis, these ideas of the movement resurfaced and other ideas like BitGold form Nick Szabo and other started moving towards and recapturing attention.

But it was the person or persons behind Satoshi Nakamoto the one who took all the ideas of this movement and made them a reality. Satoshi Nakamoto said in an email "I have been working on a new electronic cash system that is fully peer to peer, with no trusted third party". The identity of Satoshi Nakamoto is a very controversial topic that we are not going to address.

Finally in October 2008 the Bitcoin paper [8] was brought into public. It is a white paper that describes the development of the cryptocurrency whose header is shown in figure 6.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Figure 6. Header of Bitcoin original paper[8].

The first bitcoin was created on January the third of 2009 and the first transaction was between Satoshi and Hal Finney, a cryptographer that helped Satoshi with the project. The history surrounding it has been very controversial and it has had links with other scandals like the so called wikileaks from Julian Assange [12] or SilkRoad, an online black market.

The Bitcoin is an encryption-based protocol utilizing a ledger called Blockchain through a consensus system. And there is where the Blockchain started its development as we know today. Also, Bitcoin has still been growing in transactions as it will be shown in its chapter and looks like it has overcome most of its initial skepticism.

The history of Blockchain is full of clouds, controversial moves, regulatory problems and illegal transactions but it should not obscure the light of the power of the tools and opportunities it opened. Maybe it will be possible to compare the history of Blockchain with the nuclear energy one, starting with some visionaries, growing with some “bombs” and developing in a cheap and useful tool.

3. DEFINITION

As [1] defines it Blockchain is a distributed, decentralized transaction ledger, saved by each node in the network, which is owned, maintained and updated by each node. It's a peer-to-peer system. No central authority manages the transaction flow. The blockchain technology allows to track all transactions to its origin.

This is just one of the multiple definitions that can be found easily searching or reading any related publication [9]. We even already have some in laws: "Blockchain technology means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless, the data on the ledger is protected with cryptography, is immutable and auditable and provides uncensored trust" is the definition made by the house bill 2417 of Arizona in its article 5.

For this study we define Blockchain as a chain of data which uses cryptography to ensure security and is saved and operated in a distributed and decentralized way. Cryptography is a key element of any Blockchain as it ensures the security and operation of the transactions, but what is disruptive is the distributed and decentralized manner.

This makes most of the Blockchain unowned and at the same time all operated and maintained by the community on it. The revolution beyond it is the lack of necessity of a trusted intermediary as the system relies on the distribution and decentralization along with cryptography to form its own trust, a new trust intrinsic to the system and the way it operates not the reputation of any particular actor. Even for "owned" Blockchains, the ones who require permission to enter the community inside is the one in charge of its operations. With this in mind, the increase in usage of a particular Blockchain will increase its trust as more users will control and secure the well-functioning of it. Instead of relying on others the Blockchain users rely on themselves meaning they have an incentive to take care of their network.

4. AGENTS IMPLIED

This section has to serve as a definition of all the actors that we use throughout the study. In a well-functioning of Blockchain as we currently know them there must be at least these agents involved:

Public key: Is the one that defines you in the blockchain. Is like an alias in a social network.

Private key: Is your password it allows you to operate in the Blockchain. Is like your sign to validate your moves.

Block: Blocks are batches of transactions like a set of transaction or data that is unify together in order to be processed or hashed and stored. A typical block contains: Magic number (Value set), Blocksize (Number of bytes that follow, until the end of the block), Transaction counter (Number of transactions in the following list), Transactions (List of transactions contained in the block) and starts with the Blockheader (Header with metainformation about the block and the chain). This header contains the version, the hash from the previous block, the hash root of the Merkle tree or hash tree, the block creation time stamp, the bits, which specifies the complexity and its own hash.

Node: Is each one in the Blockchain also known as miners. Mining is key as they take a block of transactions, use their resources (typically energy), solve the problem to conform a hash, reach consensus and save a copy of the chain. They are in charge of the operation and maintenance of the Blockchain. Nodes come and go but the overall increase on them means an increment of security and reliability.

Hash: is the key in the cryptography under Blockchain. It is the result of a complex mathematical problem that given a series of data produces one number. Hashing is the process by which a string of data of any given length is converted into a different string of a fixed length, called a hash. No two messages can have the same hash and the hash. The good thing is that the hash takes into account all the data in the block and so if anything is changed for small as it looks it makes the number change drastically and therefore it will produce an immediate alarm to the system. In Figure 7 we

can see how hashing interlace the data referring to itself making any change alter all the following hashes and making the network deny that block.

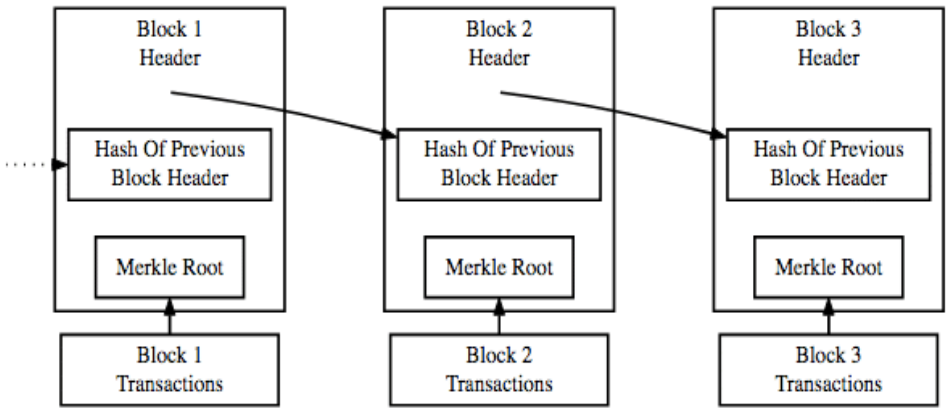


Figure 7. Graphical description of hashing [13].

Cryptographic algorithm: Is the algorithm that determines how the hash is created given a set of data.

Consensus mechanism: is the mechanism by which the transaction is verified and accepted to form a new and valid part of the Chain. Even there are other combinations and different specifications like the one proposed in [14] here we present 5 main types:

Proof of work: It was the first one to appear with Bitcoin. It consist in launching the blocks to make the miners compete against each other to be the first one solving the hash of the block. This work, the hashing, is costly and therefore disincentives the return obtained by altering the transactions.

Proof of stake: Consist in an algorithm that selects as a function of the stakes in the blockchain who would mine the hash of the block. As [15] explains unlike the PoW, where the algorithm rewards the miner who solves the problem in order to validate transactions and create new blocks, in PoS the creator of a new block is chosen deterministically, depending on its wealth, also called stake. Then there is no reward. So the coins are created in the beginning, and this number never changes. In this situation the miners are not rewarded with new coins but receive the coins from the transaction fees. That's why miners in PoS systems are called forgers.

Proof of activity: it is a hybrid model that consist of combining the previous the previous two. As [16] explains “PoA protocol seeks to

decentralize the power that synchronizes the transactions in a quite pronounced fashion". In a first phase it works like the PoW but the final transaction is hashed by a PoS mechanism.
Proof of capacity: it consist on gaining rights to maintaining by opening storage capacity to the Blockchain. In [17] explains that this is a new protocol with low usage that is intended to democratize more the access to mining as Hard disc storage is cheaper than processing power and diminish the consumption of energy.
Social: Other Blockchains use a system of social consensus where each node can recommend a number of new and trusted nodes. In that way the network is constructed biased by the participants. It bases its trust in the will of the nodes to ensure the well-functioning of the whole network.

Public vs permissioned: As the name clearly differentiates between them in public ones everyone can have access to the ledger or become a node while in permissioned Blockchains there are restrictions. These limitations affect either in the main access to the network or in the consensus mechanism participation. Permissioned Blockchain are a special matter when privacy plays a crucial role and have taken special interest from the financial world [18].

Token vs token-less: A token is the unit of measurement and reward of a Blockchain. Sometimes it is confused with the own Blockchain. In the modern cryptocurrencies a Blockchain system is just implemented to support a token. As described in [19] Token-less blockchains are simply mutually distributed ledgers where time tamping/consensus/cryptography mechanisms are used to verify/store/share data more efficiently and automate processes. A Bitcoin is a token that has its Bitcoin Blockchain and its own technical specifications that makes the Bitcoin the token has its own properties and functioning. Tokens itself are hype, regulators do not agree if they are assets, securities etc. but its acceptation and the claims of pure speculation on them have created a huge popularity.

5. SMARTCONTRACTS

SmartContracts are what is called the second generation of Blockchains. As it is developed in [19] SmartContracts are simply a computer program with some embedded logic, but when inside a blockchain, they can decentralize and automate processes. Basically, it work by adding logical propositions to the transactions. As we know all automation requires a certain logic and so SmartContracts is the form of combining the benefits of Blockchain to the world of automating process and ensuring trust on them.

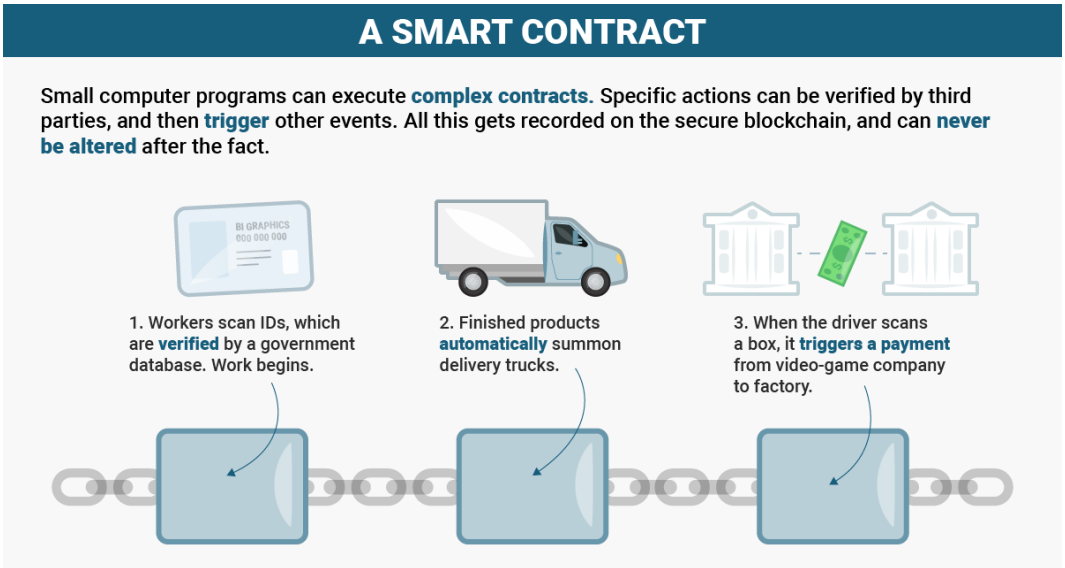


Figure 8. SmartContract explanation [20].

As figure 8 exemplifies, the possibilities of adding logic to the Blockchain in the way of SmartContracts opens a world of possibilities for automating purposes. Also, it has some technical issues with relation to the coding (preventing that no script can be looped etc.) as discussed in [21]. This reflects that there is the need to ensure that scripts have always an end because if it enters an infinite loop it will damage the rest of the process and transactions the Blockchain is in charge.

i SOLIDITY

The appearance of SmartContracts has come also with a new programming language called Solidity. This language is just used for SmartContracts.

Figure 9. Solidity Logo.

Even this types of contracts can be written in any language, supported by the platform, solidity is a contract-oriented solution that optimizes the writing and execution of this pieces of code [22]. It is also a language that is statically typed which means that the type of the variables are known at compilation. Moreover, it avoids some bugs that may arise later as the checking is doing in compilation.

6. INITIAL COIN OFFERING

Another important term to have in mind, when surfing the Blockchain world, is the term ICO's. It responds to the naming of this chapter. Initial Coin Offering is not more than pre-selling tokens to the public as a way to fund the organization behind it.

ICO's are not a part of the Blockchain technology but are a mechanism that can be used to fund and to start creating acceptation to it. Further, is a very controversial subject because of the unregulated state in which they are and other claims such as speculative character of themselves. However, according to [23] it is undeniable that their renown has grown even the fall of the majority of the trials as it shows Figure 10 that the money invested by this channel has kept growing.

Figure 10. USD raised by ICOs [23].

7. HOW BLOCKCHAIN WORKS?

There are lots of guides, articles and publications that conceptualize and/or exemplifies the work of a blockchain, from the basics [25] to a more complete view [26]. In this section we try to summarize and simplify with a technical perspective the functioning of a blockchain.

For that purpose, we stablish three points of view: actors in the transactions, miners and developers. We do this because focusing ourselves in the three main possible places that the technology offers us a complete view of works the environment as a whole.

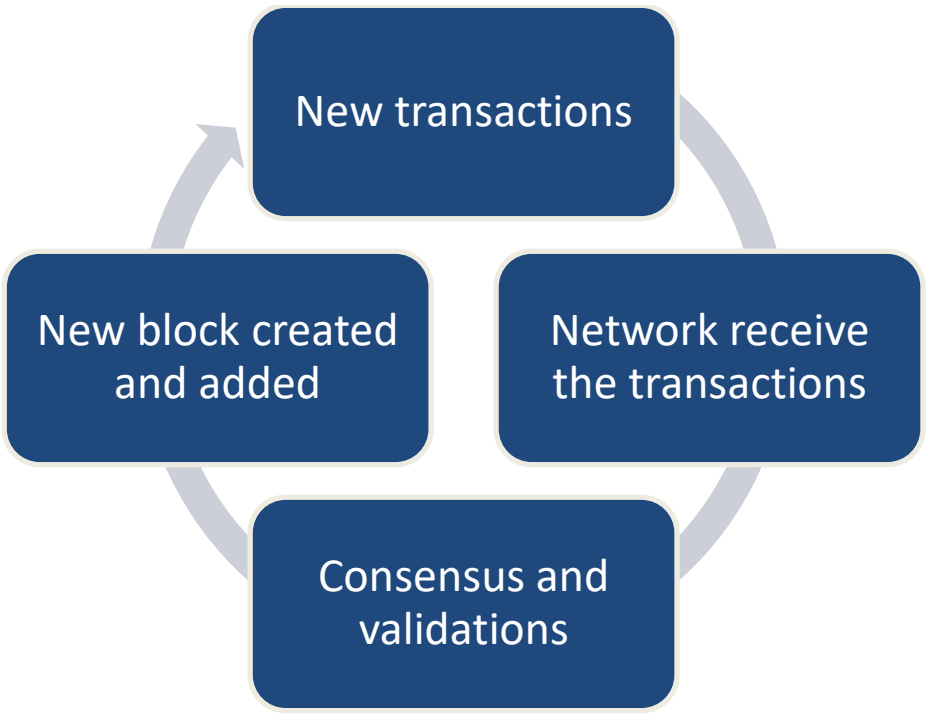


Figure 11. Blockchain process.

When a transaction wants to be made, the actor/agent has to know the public key of the ones she wants to send the transaction for. In order to validate it she has to sign that transaction with your private key. Any transaction going out of an account needs to have the recipient's public key and the sender's private key regardless if it

has been processed directly or after the code of SmartContract decides it. After that the transaction is sent to the distributed network of nodes for consensus and validation. There is where miners appear in scene to create the trust and correct the mistakes to end with a valid block. When that happens, the transaction is completed and the block that contains it is created in the blockchain following the previous one and creating a chain of blocks. This transaction cannot be undone or erased of the blockchain and is publically known for anyone who has the access to it.

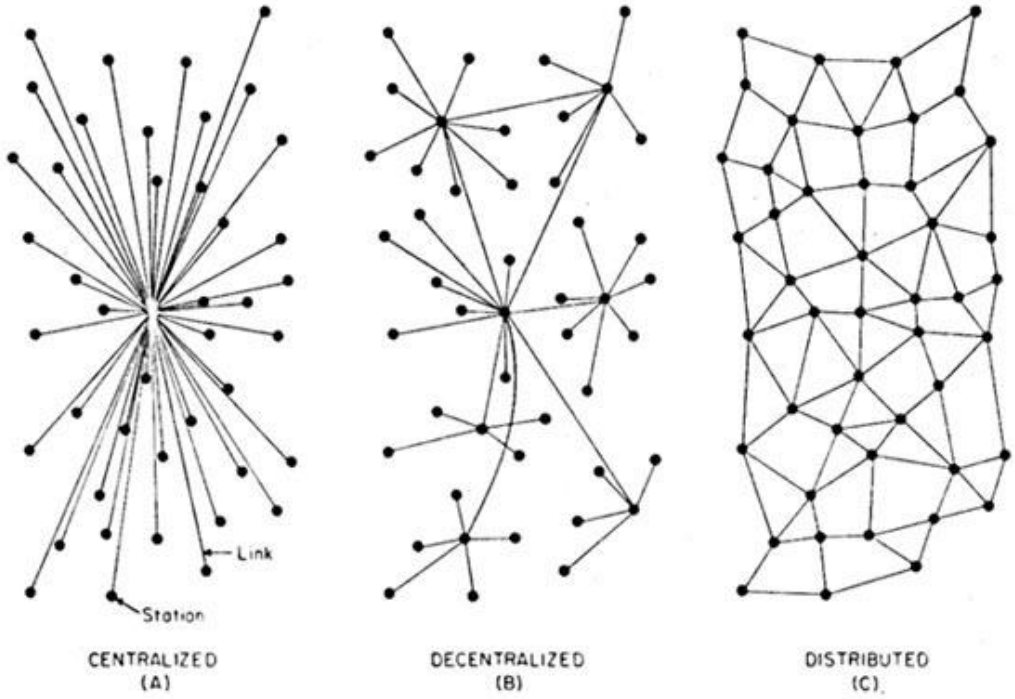


Figure 12. Network typologies [27].

In figure 12 we can see that transactions between accounts of the same financial institution will have a centralized network were trust is based on the central node. Decentralized network can describe the banking system or a supply chain with different intermediaries where trust is single relation between each node that communicates or transacts. Finally a distributed network like the ones Blockchain presents the trust is a shared goal of all the network and all or the amount selected deterministically create trust by consensus.

Miners, forgers or validators are the ones in charge of the process of receiving the transaction and seal them in to the blockchain. This process can happen in multiple different ways as we have explained in the point of the consensus mechanism of chapter 4. Also, to become one it depends on whether the Blockchain is public or permissioned. This process can be rewarded or not. Miners usually hash the transaction and safe a copy of the Blockchain but there are networks where this roles are different. Finally, taking outside the financial profit that can be obtained by miners, their goal is to cooperate or compete to maintain the trust and the operation of the network.

Finally, developers have in blockchain another tool that has increased their possibilities. From creating a new Blockchain initiative to wallets that allow an easier use of the existing ones to Smartcontracts, decentralized applications and even autonomous decentralized organizations the range of possibilities brought by this technology is huge as shown in figure 13. Some of this possibilities will be explain in the next chapter.

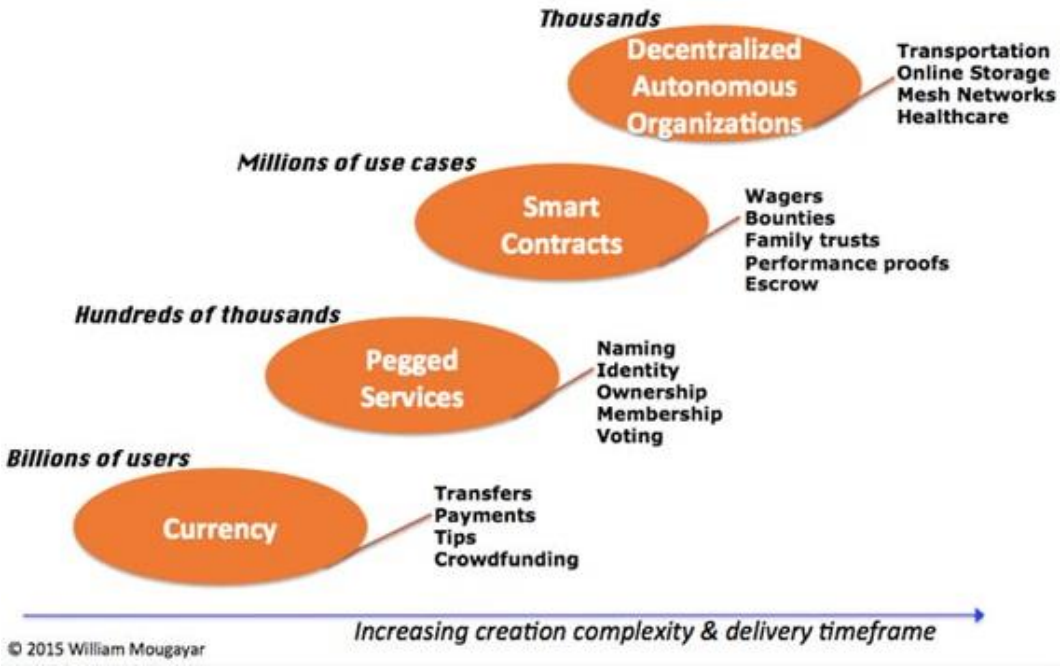


Figure 13. Blockchain developing possibilities [29].

8. *FRAMEWORK*

There is a theory that assumes true Blockchain to be a specific use of it leaving outside this truth permissioned or non-tokenized uses. In figure 14 [30] it is shown how "true blockchain" maximizes in all axis. However, it arguable that transparency and security cannot be reached as anonymity does not help to prosecute crimes.

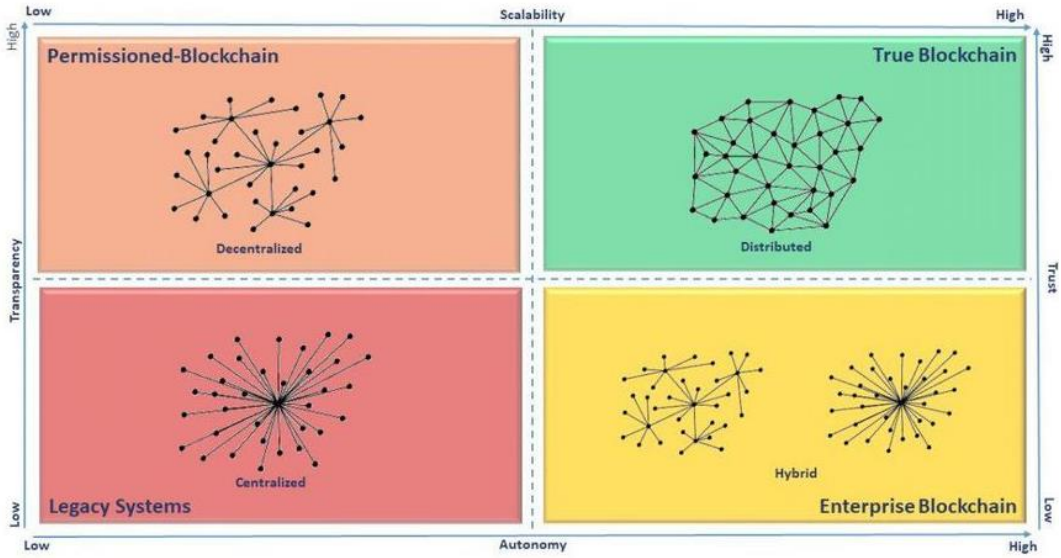


Figure 14. True Blockchain theory [30].

But using the given definition in chapter 3 Definition and attending to the reality that it is being used in many forms and with different specifications we want to be able to analyze of all its. Against these ideas of a true Blockchain this study comes with a goal of creating a framework to analyze the different uses that this technology can take. This comes by taking into account that there is not one medicine for all disease and that a permissioned-Blockchain can be a better solution than a public one (that is what some call true one).

This has result in a blank business card that leaves the proper places and spaces to allow the user understand what technology is beyond each of the Blockchain initiatives and what are its main features. The plain framework is presented in Figure 15.

name						[day/month/year]
Public	**Permissioned**	**Consensus mechanism**				
		Detail:				
		PoW	**PoS**	**PoA**	**PoC**	**Social**
SmartContracts		**Protocol:**				
yes	**no**	**Version:**				
		Cryptographic algorithm:				
token	**token-less**	**Block size:**				
		Generation time:				
name:		**Blockchain size:**				
USD value:		**Detail:**				
Detail:						

Figure 15. Framework blank.

With this Framework we will analyze some uses of Blockchain and determine at first sight the consensus mechanism, its overall possibilities (SmartContracts) and limitations (Public vs Permissioned) and other technical details of interest. It also have the spaces to include some practical explanation of the main topics analyzed by the framework.

It is supposed to serve as presentation card in order to compare one technologies to others and to get a fast understanding to someone familiarized with the different agents that take part of the landscape.

9. BENEFITS

Here we develop the main benefits that Blockchain networks can bring to business and people. We will not enter into considerate ideological benefits related to libertarian thoughts though we do not deny their existence. Although such benefits have an important business and developing branch, there is another, related to ideological benefits. Hereon, we focus our attention to the economic and social ones.

Financial institutions were the first ones to be impacted with the security and speed promised by Blockchains. First of all, the cryptocurrencies shocked them but as we can see from [28] they are starting to use the same technology to counter attack. In [31] we can see how numerous cost saving procedures can be affected this technology in the field of asset management as a particular case. Also shown in this report, the settlement of transactions between banks (the ascertainment and transference of funds) is identified to cost the financial industry anywhere from $65-$80 billion a year

Other companies are embracing these possibilities and, according to the literature, have special impact on supply chain [32] and healthcare [33][34]. In the next chapter some examples of applications will be shown. But mainly all digital actions can be disrupted as in [35] that we can see how human resources will be benefited from Blockchain networks.

Governments and other public institutions that act as trusted third parties can take advantage of Blockchain to improve their services to society. Blockchain can improve trust and avoid corruption [36] or create a unified and secure land register [37] and the list goes on and on.

To summarize the positive social opportunities Blockchain brings to the table it is interesting to see the words of the UN's Sustainable Development Goals, Blockchain Commission for Sustainable Development [39] that "envisions the development of radically creative decentralized solutions to issues including:

conservation of natural resources, protection of the commons, economic growth, empowerment of all communities, financial inclusion and security, public health and welfare, civic trust and protection of the integrity of democratic systems—among others—for the benefit of our common humanity". And also the UN organism highlights that this technology should not be seen as a threat but as an opportunity.

To summarize the business opportunities with Blockchain technology, IBM proposes [38] the five most important benefits:

- More transparency
- More security
- More traceability
- More efficiency and speed
- Less costs

10. TECHNICAL CONTROVERSY

In this Section, we will speak about some technical variables on controversial topics surrounding the Blockchains networks. A whole chapter can be made on the different regulations especially on cryptocurrencies but we will leave it as it goes outside of the scope of this study. All the agents implied in a Blockchain are subject to some controversy as ones think there is better one consensus mechanism or other or one algorithm or the other. We discuss here:

Hard Forks and soft forks: These are changes in the protocol of a blockchain that require the nodes and users to update [40]. A hard fork creates different paths on the blockchain as shown in figure 16 while a soft one where the blockchain still in one path but the protocol has suffer some changes/improvements The problem and the opportunity with forks is that it can invalidate transactions as the new chain can before blocks already validated. This opens the possibility to undone massive hacks [41] but can also reduce trust in the network.

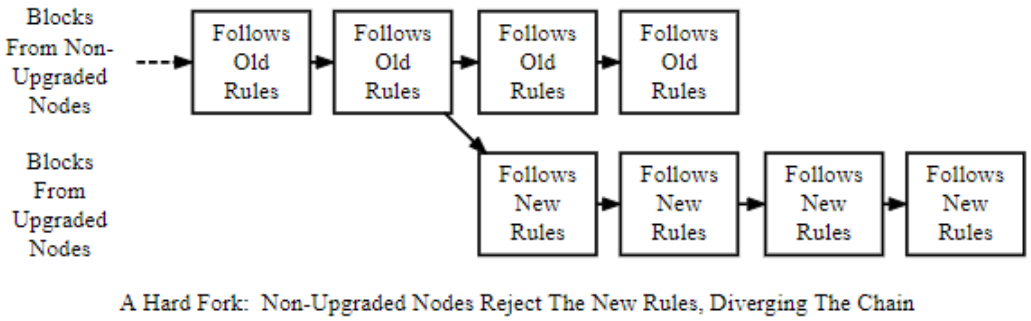


Figure 16. Hard Fork diagram.

Time to generate a block: Another major controversy comes with the time gap between validations in a Blockchain. As we will see later in some examples times can go from 10 minutes (Bitcoin) to 3,5 seconds (Ripple) and there are arguments in favor of both fast and slow time. There is a lot of discussion in the communities of developers, miners and users of the best solution [42] and there are famous Blockchainers like Vitalik Bulterin – Founder of Ethereum- making propositions [43]. Here we are not going to impose a perfect time but give an overlook of the pros and cons of each option. Shortening the block time will give faster confirmation time to the transactions and more chances or less variance in the validating nodes to process transaction as there are more opportunities and the difficulty decreases. On the other side, nodes will have to increase their bandwidth to be able to communicate properly, it will increase difficulties in case of forks and the security is decreased as it is easier to attack with a lesser difficulty.

Electrical consumption: When validating transactions Blockchains nodes have to use resources especially electricity. There are some articles arguing that bitcoin alone consumes more electricity than 159 countries [44] as well as some others that critic these kind of catastrophically affirmations [45] but what is clear is that there is a great debate. Supporters argue that it is a matter of time of technological development as well as a market issue (more people will try to hash as the market value of prizes increases) and detractors say it is not sustainable. It is clear that most development has been followed by an increase in power consumption and that sustainability is a big challenge. Furthermore this fear comes mainly from the demands of the mechanism of proof of work (the one Bitcoin uses) and we have seen that the technology is currently creating different solutions to the consensus mechanism that can avoid a huge world competition in mining without losing too much in the security side.

Chapter 3 WHERE IS BLOCKCHAIN USED?

1. INTRODUCTION

In this chapter we will speak about the main places where Blockchain is used. We want to present a complete Outlook to the reader of the most interesting and renowned uses that have Blockchain in its core.

For that purpose, we firstly speak deal with cryptocurrencies, which is the developer of the technology and the most famous use, taking a closer look to Bitcoin as its frontrunner. Then, we take a look into Ethereum as a platform for Blockchain and the most remarkable example for SmartContracts and future developments. After that, we examine how the energy sector is trying to adapt and take in this technology. Finally, we will highlight some business models that are being developed to exemplify the multiple uses this tool have to bring to the table.

The idea of this part is to take all the concepts learned previously to the real world and to dissect the different alternatives and uses this technology has. As a part of the motivation of this study this chapter answers the aim to show the disruptive power of Blockchain.

The concepts explained in the previous chapter are key to understand this one. Also we use the framework created to evaluate the different Blockchains here described.

2. CRYPTOCURRENCIES

We start with the definition made by [46] of cryptocurrencies: *"digital or virtual peer to peer currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation".*

However, for us this definition is too broad and leaves space to other multiple studies that do not subscribe to the matter of this study. That is why we just treat them with the limitation of subscribing Blockchain.

Cryptocurrencies have grown heavily lately as shown in figure 17 and they have their unique features and that is why they deserve to be treated separately.

Figure 17. Cryptocurrencies market capitalization [47].

In this section we will highlight specially to Bitcoin, because of its history that made it the initial model for any cryptocurrency and all the Blockchain ecosystem. After that we will talk about some of the other ones that are also an important part of the current landscape.

ii BITCOIN

The history of Bitcoin has been summarized in chapter 0. To analyze it we start with the framework previously created in chapter 8 Furthermore, we proceed with the foundational white paper and finally, we talk about some market issues to highlight its importance and reach.

In figure 18 we can see the framework filled for the Bitcoin. It highlight that is a pure proof of work as a consensus mechanism and it is a public network, also more technical details can be found on it. The protocol is an own bitcoin protocol for reference client standardized from C99 standard [48] and *getblocktemplate* for mining.

Bitcoin [11/06/2018]						
Public	**Permissioned**	**Consensus mechanism**				
✓	×	**Detail:** Pure proof of work				
SmartContracts		**PoW**	**PoS**	**PoA**	**PoC**	**Social**
yes	**no**	✓	×	×	×	×
×	✓	**Protocol:** Bitcoin for reference client . Getblocktemplate for mining				
token	**token-less**	**Version:** Bitcoin Core version 0.16.0 2018/02/26				
✓	×	**Cryptographic algorithm:** SHA-256 and RIPEMD-160 for addresses				
name:	Bitcoin	**Block size:** 1 MB average 595.312 Kbytes				
USD value:	6,722.84	**Generation time:** 10 minutes				
Detail: Most important cryptocurrency		**Blockchain size:** 201.04 GB				
		Detail: Bitcoin is the most famous cryptocurrency and the one with most adopters as well as market value and single value with relation to forex and developer of the first Blockchain and its technology and principles.				

Figure 18. Framework for Bitcoin.

With a clear overview of what Bitcoin is, we are now going to analyze the foundational white paper Satoshi Nakamoto wrote [8]. It starts summarizing the soul of the proposition a lot of reflexing about third party trust and its costs. It speaks about: “inherent weaknesses of the trust based model”. In this start is where the cypherpunk movement principles are reflected. After that it enters in the functioning of the system with hashing system and time stamped server and the proof-of-work to ensure transactions. For further information about the working there explained recap to the chapter 7 and add the knowledge of proof of work as the consensus mechanism. There, it is remarked that Bitcoin does not allow

SmartContracts but with UTXO a "weak version" of them can be maid but we will leave a no as it is not fully intended to it.

Once the system is mainly explained, it enters in one of the other main dilemmas, the spaces on disk and the evolution of transactions and their sustainability throughout the time. It results interesting the original explanation: *"If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory"*. Finally, it stablishes the calculations to attack the chain and concludes that *"becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power"*.

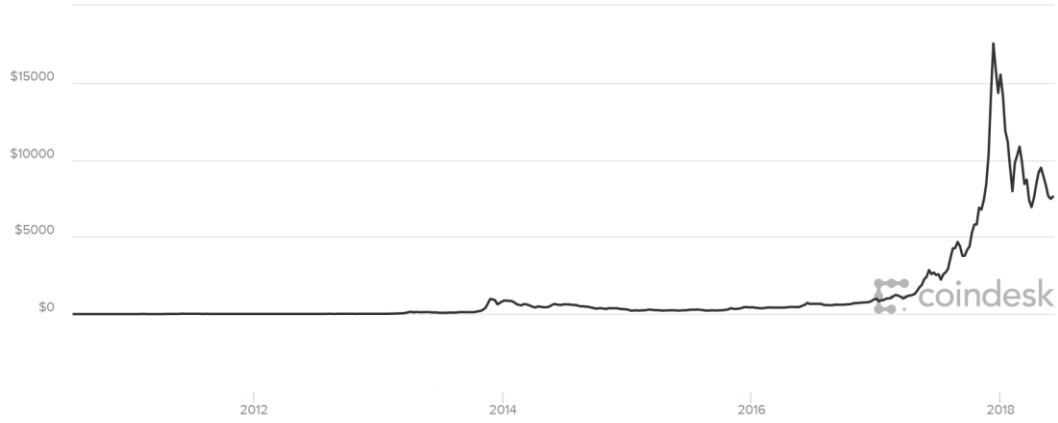


Figure 19. Bitcoin to USD evolution [49].

To understand the importance Bitcoin has taken it is sufficient to take a look to figure 19. In it we can see how Bitcoin started with 0.06 US Dollars and peak at more than 19.000 US Dollars for one Bitcoin at the end 2017. Outside the figure, the price has recently fallen hugely to return to values of mid 2017 having ended the speculator cycle represented in the peak.

iii OTHER CRYPTOCURRENCIES

Bitcoin represents the maximum actor of the cryptocurrencies' landscape. With it Ethereum shows a strong performance and will be treated in a separate section due to its importance. There are lots of cryptocurrencies but we will analyze just some examples.

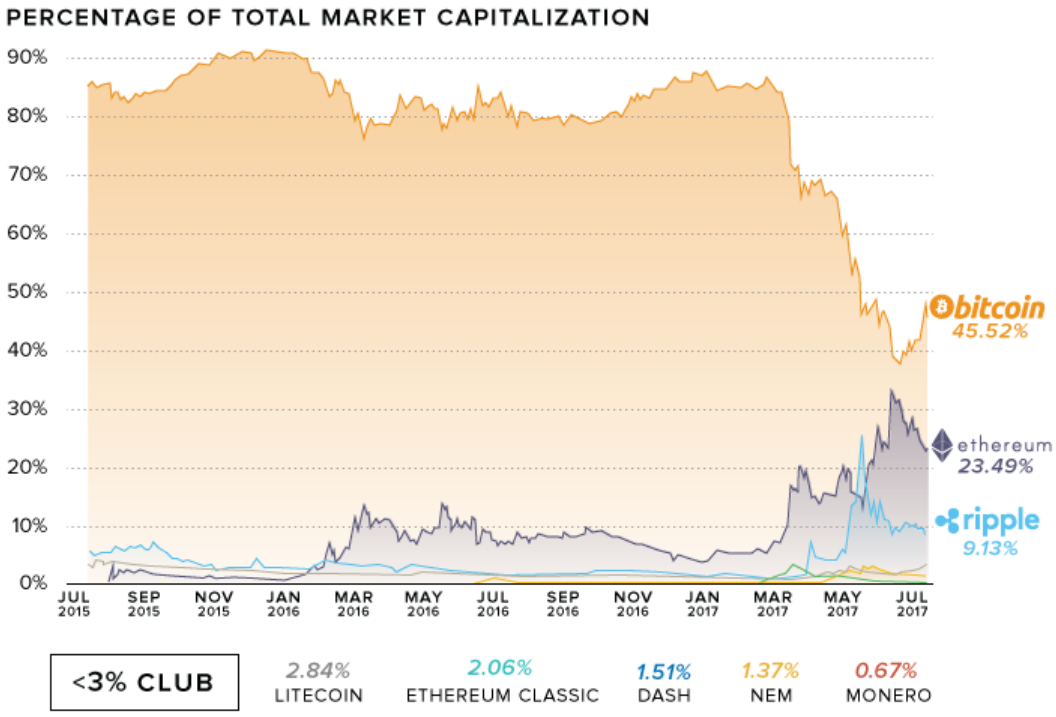


Figure 20. Cryptocurrencies: percentage of importance [47].

In order to analyze another two samples, Figure 20 shows us that Ripple and Litecoin are clearly playing an important role to investors and are the two most valuated besides the previously mentioned.

As far as we know, the world of cryptocurrencies is really vast and dynamic, so we left for further works to address tons of other technicalities that differ from each of them. Some other interesting examples can be Burstcoin which uses Proof of Capacity as a consensus mechanism or more polemic topics as the possibility mentioned by the press that Catalonia could create a cryptocurrency to prepare its separation from Spain [50].

Ripple

As itself is described [51] Ripple is "The world's only enterprise blockchain solution for global payments". The protocol supports a payment method based in its own cryptocurrency with the same name. The developers behind this project are a company with profit expectations that joins lots of big financial institutions that help in the support and development of the network, some of the ones that they highlight in their web are shown in figure 21.

Figure 21. Ripple global network sample [51].

Ripple is a particular case of cryptocurrencies mainly because is the one that shows the reception of the financial world to the technology. It is a permissioned network and uses a different way of consensus mechanism to the traditional proof of work. As can be seen in the framework in Figure 22, is not just a permissioned network but also there is a lot of information that cannot be found due to this privacy. However, it is very interesting to see how the traditional world is embracing the tools developed by cyberpunks.

Ripple [11/06/2018]						
Public	**Permissioned**	**Consensus mechanism**				
✗	✓	**Detail:** Unique Node Lists. Validators a participant believes will not defraud them				
SmartContracts		**PoW**	**PoS**	**PoA**	**PoC**	**Social**
yes	**no**	✗	✓	✗	✗	✓
✗	✓	**Protocol:** Ripple transaction protocol				
token	**token-less**	**Version:** Rippled v1.0.0 2018/05/31				
✓	✗	**Cryptographic algorithm:** Ripple Protocol Consensus Algorithm. Ed25519 for address				
name:	XRP (Ripples)	**Block size:** n.a.				
USD value:	0.571	**Generation time:** minimum of 3.5 secs				
Detail: The 100 billion Ripple coins were created at launching.		**Number of tansactions:** n.a.				
		Detail: Ripple is mainly thought to big financial institutions, its cryptocurrency is tradable in open markets but the access to the network is limited. The Consensus mechanism has no rewards and relies on the willingness of the nodes to maintain it.				

Figure 22. Framework for Ripple.

The consensus mechanism used by Ripple differs from the classical mining in public network is seen in figure 23 and described [52] as *"The nodes that receive, relay and process transactions may be either tracking nodes or validating nodes. Tracking nodes' primary functions include distributing transactions from clients and responding to queries about the ledger. Validating nodes perform the same functions as tracking nodes and additionally contribute to advancing the ledger sequence"*.

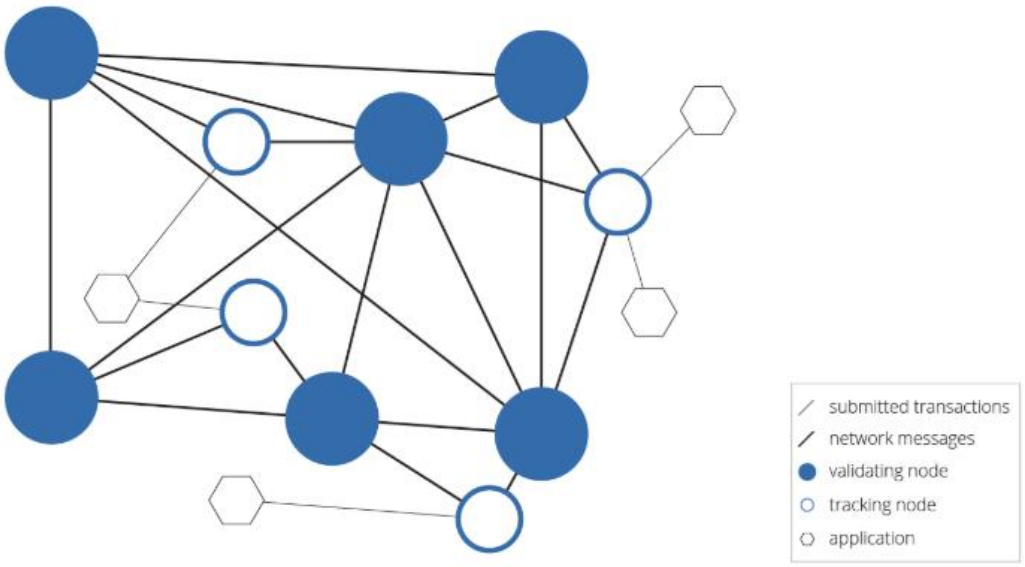


Figure 23. Participants in the Ripple ledger [52].

As we have seen in figure 22 in the framework the speed of generating a block is much higher in Ripple than in any other network that is due to and a consequence of the iterative process used to a single transaction explained in figure 24.

The lifecycle of a single transaction is as follows:

- A transaction is created and signed by an account owner.
- The transaction is submitted to the network.
  - Badly formed transactions may be rejected immediately.
  - Well formed transactions may provisionally succeed, then later fail.
  - Well formed transactions may provisionally fail, then later succeed.
- During consensus, the transaction is included in the ledger.
  - The result of a successful consensus round is a validated ledger.
  - If a consensus round fails, the consensus process repeats until it succeeds.
- The validated ledger includes the transaction and its effects on the ledger state.

Figure 24. Transaction lifecycle for Ripple [52].

Litecoin

Litecoin is a cryptocurrency known as the silver of its world. It is technically nearly identical to Bitcoin. As [53] explains was created by Carlie Lee, former Google employee, in October 2011 as an open source project. Two main changes were made to the Bitcoin protocol: increasing the speed of transaction validations by 4 times; and the cryptographic algorithm changed from SHA-256 to Scrypt to allow more nodes to access the network as miners.

Litecoin [11/06/2018]						
Public	**Permissioned**	**Consensus mechanism**				
✓	×	**Detail:** Pure proof of work				
		PoW	**PoS**	**PoA**	**PoC**	**Social**
SmartContracts		✓	×	×	×	×
yes	**no**	**Protocol:** Litecoin opensource				
×	✓	**Version:** Litecoin Core v0.16.0 2018/05/31				
token	**token-less**	**Cryptographic algorithm:** Scrypt and RIPEMD-160 for addresses				
✓	×	**Block size:** average 33.306 Kbytes				
		Generation time: 2.5 minutes				
name:	Litecoin	**Blockchain size:** 17.27 GB				
USD value:	105.18	**Detail:** Litecoin is basicaly the same thing technically as Bitcoin but differs on the speed transactions are added to the ledger which is 4 times and the Algorithm used for the hashing that is said to suit less powered nodes				
Detail: Litecoin is said to be silver as bitcoin is gold						

Figure 25. Framework for Litecoin.

As we seen in this cryptocurrency appears one of the most important factors of technical controversy that we spoke about in chapter 2 section 10 of reducing the time for the block generation.

3. *ETHEREUM*

As mentioned in the Harvard Business Review [54] "Blockchain applications will move beyond finance" and Ethereum is the platform that reflects this changes in direction. In figure 26 we have the main technical information of the Ethereum platform which allow its tons of uses.

Ethereum [14/06/2018]						
Public	**Permissioned**	**Consensus mechanism**				
✓	×	**Detail:** Proof of work but programmed to change to Proof of stake				
		PoW	**PoS**	**PoA**	**PoC**	**Social**
SmartContracts		✓ →	×	×	×	×
yes	**no**	**Protocol:** Ethereum protocol				
✓	×	**Version:** Ethereum Streamline v1.8.11 2018/06/12				
token	**token-less**	**Cryptographic algorithm:** Ethash based using Keccac (SHA-3)				
✓	×	**Block size:** 25.448 KBytes				
		Generation time: 14,9 seconds				
name:	Ether	**Blockchain size:** 667.10 GB				
USD value:	515.85	**Detail:** Ethereum is a public blockchain that provides a distributed computer platform and an operating system to run smartcontracts. The cryptocurrencie asociated with it (ethers) serves as the fuel/payment to operate inside the platform.				
Detail: Ether is the gas to operate in the platform						

Figure 26. Framework for Ethereum.

Ethereum is the platform that concentrates the most initiatives to implement new projects in the Blockchain. As it is an open source all the decisions on it have to be approved by its users and there is expected to change to a Proof of Stake in 2018 in it version code named Metropolis (vConstantinople) as commented by the Ethereum Team [55].

Its token called Ether is the payment for all the activities realized on it. As stated in the Ethereum yellow paper [56] the fees, or how they call it gas, can be charged in three different scenarios of operation:

- Intrinsic to the execution of an operation
- As form in a payment for a subordinate call or a contract creation
- An increase in the usage of the memory

The network allows to run SmartContracts (explained in Section 5) and have its own language for the coding called Solidity. These SmartContracts open the door to two new concepts: DAPPs & DAOs.

i DAPPs & DAOs

The initial of DAPPs correspond to the terms: Decentralized Applications and Decentralized Autonomous Organization. These two terms are the most important uses of SmartContracts and the differentiation on the value proposition of Ethereum.

For an application to be considered a Dapp [57] it must meet the following criteria:

1.- The application must be completely open-source, it must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.
2.-The application's data and records of operation must be cryptographically stored in a public, decentralized blockchain in order to avoid any central points of failure.
3.-The application must use a cryptographic token which is necessary for access to the application and any contribution of value from (miners / farmers) should be rewarded in the application's tokens.
4.-The application must generate tokens according to a standard crytptographic algorithm acting as a proof of the value nodes are contributing to the application.

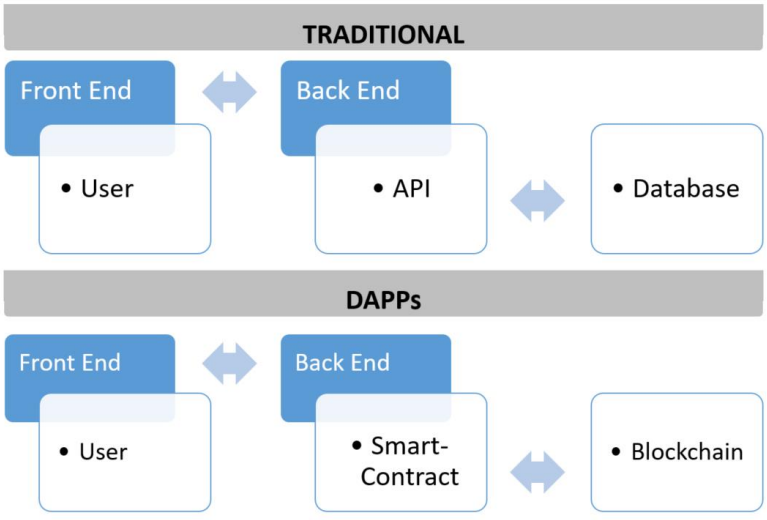


Figure 27. Decentralized Applications vs Traditional.

Decentralized Applications are considered the make use of the public/open mentality that created blockchain to the world of applications and their interaction with users. In figure 28 we can see the difference between traditional application working and the Decentralized ones based on the Blockchain. Basically DAPPs allow the user to access an application that gives access to the conditions proposed in a SmartContract. If the conditions predefined are matched the SmartContract activates the outcome pre-stablished and saves the changes in the Blockchain. For example one State can create a DAPP to give funds to farmers in times of droughts. The farmer will enter the front end and if it satisfy the demands stablished on the contract money will be transferred to his account. This will allow more control from the national treasuries as the SmartContract can access digitally to the record of rains of the national meteorology agency and just give money if the droughts are real.

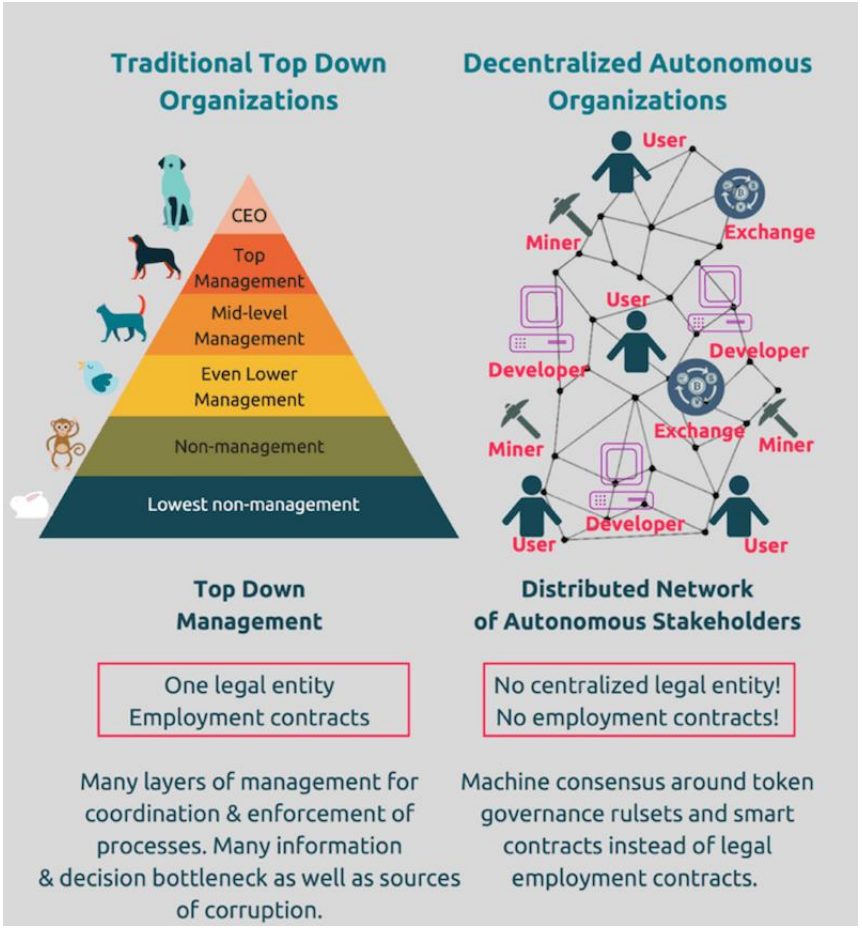


Figure 28. Decentralized Autonomous Organization vs Traditional [59].

As defined by [58] "A Decentralized Autonomous Organization (DAO) is a computer program, running on a peer-to-peer network, incorporating governance and decision-making rules. DAOs can be programmed to operate autonomously, without human involvement, or the code can provide for direct, real-time control of the DAO and funds controlled by it".

In figure 28 we can also see the difference between hierarchical traditional organization and the ones ruled by a set of SmartContracts that stablish the behavior of the different agents. This implies that the organizations must be able to measure the different contingencies digitally in order to be able to activate the SmartContract that will act as the legal document between parties and the payer.

4. BLOCKCHAIN IN THE ENERGY SECTOR

According to [60] there are presented four possible uses of the Blockchain in relation to the energy sector:

I.-Decentralized storage of transaction data increases security and ensures greater independence from a central authority.
II.-Blockchain technology has a wide range of uses; Blockchains can help to make payments via cryptocurrencies, to digitize contracts, to manage digital content, to verify transactions, to execute trades or be used in many other areas. The next big development step is expected to involve smart contracts.
III.-New decentralized business models no longer require third-party intermediaries
IV.-Whether the technology will succeed will be determined not only by the technical capabilities of the system but will also be dependent on the applicable regulatory and legal framework, the technology's scalability and resilience as well as the economic viability of investments.

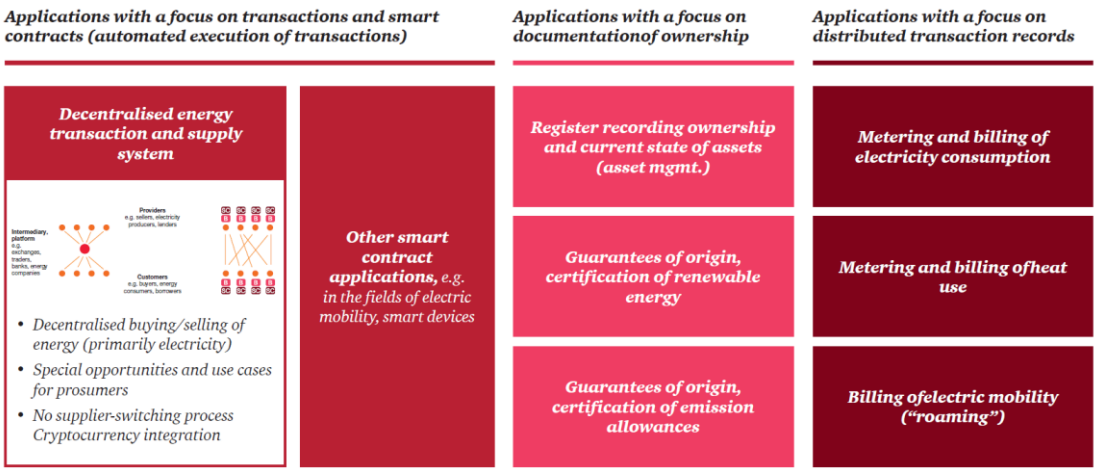


Figure 29. Overview of possible blockchain use cases in the energy sector [60].

In figure 29 it shows that there are 3 main areas of application of Blockchain in the industry. First the ones on transactions, where SmartContracts can act automating all transactions from the elimination of the central regulator to energy transactions of vehicles in cities. Also document ownerships where sellers can validate that the

energy transacted is from renewal sources or other traceability issues. Finally, as we have commented Blockchain can keep the records of transaction secured in a distributed ledger.

Transparency, security and cost saving are the major takeaways this technology can brought to the energy sector. As [61] presents "some companies have estimated potential savings in the range of 30–60%" making Blockchain a game changer technology for the sector.

In the study for the World Energy Council of Blockchain [62] it is presented that *"93% (of interviewees from the report) think that blockchain will be able to disrupt the functioning of the industry and contribute toward accelerating the speed of the changes taking place in the energy system such as decarburization and the move to more decentralized energy sources. And they are fairly bullish about the likely timescales with 87% anticipating that the most disruptive impact is less than five years away"*.

Also this article presents some of the companies and initiatives in the sector and talks about the different benefits and obstacles the technology will have in relation with this sector. In figure 30, it shows that the most important benefit is the disintermediation which will lead to new and more optimal ways to interact in the market without the need of a supervisor. Also it is interesting to see that the obstacles reflect the maturity of the technology (there are not proven suppliers of services or knowledge) and the uncertainty behind it.

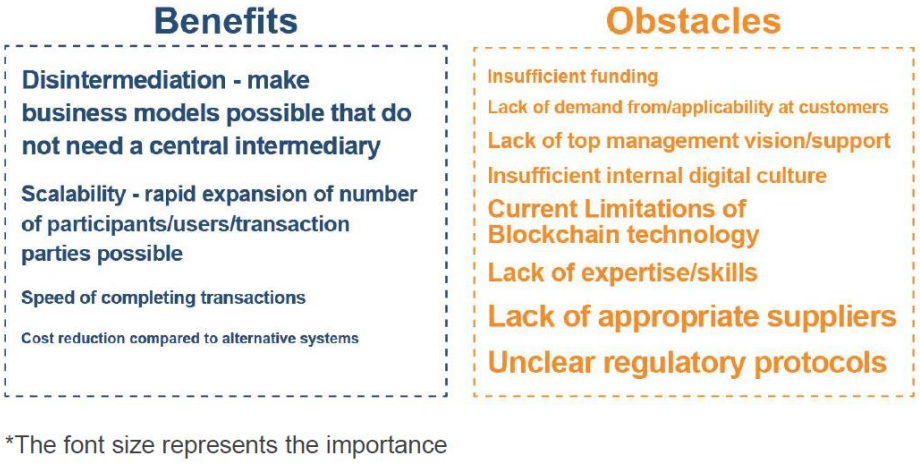


Figure 30. Benefits and obstacles of Blockchain in the energy sector [62].

i ACTORS OF THE ENERGY MARKET

The Blockchain technology is said to disrupt all the value chain of the energy production to consumption, and companies and initiatives are starting to take positions as we can observe in Figure 31.

Figure 31. Blockchain stakeholder activity in the energy sector [63].

First of all, Peer to peer trading and connected home startups allow consumers to share energy between themselves, manage energy storage or different consumptions in the area of Internet of things. Regarding the growth of Electric Vehicles and the necessity to increase the points for recharging there are companies taking positions to manage that flows. There are also nodes created to serve as consortia and research to increase the visibility and knowledge of the technology. Bitcoin and other cryptocurrencies are aimed by some stakeholders to serve as a payment method to utilities. There are initiatives that have created solar cryptocurrencies that meliorate the utilization of solar energy. Also the disintermediation of the market regulator can be done with Blockchain, and the term smart market is being created to call the automatization of it.

5. *BUSINESS MODELS WITH BLOCKCHAIN*

From retailers to cloud companies from Oceania to California Blockchain is being introduced in new type of business models. There are a lot of examples where Blockchain is implemented as the foundation to transform business structures. According to [64] there are 10 industries that have high possibilities of being disrupted by blockchain. In figure 32 we present a summary done to exemplify initiatives on those sectors.

Industries	Overview	Examples	Explanation
Banking	First applications. Double spending solution. Banking records (faster and cheaper).	Bitcoin	Criptocurrency that serves as a substitute for money.
		Ripple	Offers solutions for global payments and aggregattes banks in it.
		BBVA	Was the first bank to issue a syndicated loan through Blockchain.
Healthcare	Access to health records from doctors secure, safe, inmediate. Without bureacracy.	Synaptic HA	Ensure that the most up-to-date information about healthcare
		GHX	Protocols to verify if a healthcare provider is licensed.
		frtyl	Service that links fertility centers with parents seeking treatments
Politics	Avoinding rigged votes, "voting irregularities", counting errors. Fastering registration.	Zcoin	World's First Large-Scale Blockchain-Based Political Election Held
		Democracy Earth	Sovereign, open source, decentralized democratic governance protocol
		Follow My Vote	Secure online voting platform to allow for greater election transparency
Real Estate	simplify property exchanges and eliminate escrow altogether. Comissions reduced.	Deedcoin	Cryptocurrency powered transactions that decrease the commissions
		Propy	smart contracts for real estate store, allowing buyers, sellers.
		Atlant	Trade tokenized property and rent apartments without paying high fees
Legal	Storing and retrieving documents as well as verifying their provenance.	OpenLaw	Automatically generate legal agreements and embed smart contracts
		Integra ledger	Permissioned blockchain to increase the integrity of legal documents.
		ContractCode	Coding platform that will generate traditional and smart documents
Security	Eliminates many of the problems of data hacks. Advanced cryptography.	Cryptyk	breaking up data into disparate parts and storing them
		Storj	Open-source project for storing and saving files
		Sia	Market of buyers and sellers of file storage by use of smart contracts
Government	Eliminate bureaucratic red tape and corruption in government agencies.	China Tax	Social taxation and electronic invoice issuance matters processing
		Zug ID	Zug city is piloting a government-issued self-sovereign ID
		DISC Holdings Ltd	A way to receive, spend and track benefit payments
Rentals and Ride Sharing	True peer-to-peer networks for rentals and sharing of goods and services	RentBerry	Rental platform tokenized
		Ridecoin	Rideshare Marketplace
		LaZooz	Decentralized, community-owned transportation platform
Charities and Aid Organizations	Trust through smart contracts and online reputation management systems	Alice	Social funding and impact management platform
		Bithope	Develop and promote charity through cryptocurrencies crowdfunding
		Give Track	Real-time financial transparency for effective philanthropy
Education	Notary for educational records. Grades and records would be easily and instantly transferable	Parchments	Order, clain, manage and verify academic records
		Indorse	Skill validation without user giving up their data
		Woolf University	Student and teacher "check-ins" to executing smart contracts

Figure 32. Blockchain sectorial initiatives exemplification.

As we have seen on the previous chapter, banking industry is been the first one generating business models based on blockchain. Some initiative have been already explained and that is why we will not cover much more of it here. Financial services is the field where the technology is at a higher stake of maturity.

The second sector we find in figure 32 is healthcare. Medical records are highly regulated and exchange between different health organizations is difficult. To benefit users and with the claim of saving lives blockchain initiatives are been developed to create a unified health record where the patient/user have the power to use and give access to her medical history. Also in figure 32 we have presented some different examples on the sector that focus on verification (traceability) and linking offer and demand of services for the sector.

In the political sector the big issue blockchain is being implemented is voting. Errors can be a thing of the past with the implementation of digital voting systems. However adding blockchain can improve robustness and authenticity of the system, eligibility of the voters, through verification of identity, as well as traceability. Also there are more ambitious initiatives to rule political life through SmartContracts to increase democracy participation [65].

In the real estate business initiatives to simplify and ensure property transactions occupy the main focus. However, there are also important initiatives that focus on financial services for the industry.

All these sectors studied present numerous initiatives as we exemplify in figure 33 for the Real estate sector Blockchain is being implemented in the value chain of most sectors. In figure 32 we have tried to show a summary and an exemplification of some notable initiatives to show the power and direction of Blockchain implementation through the different sectors of the economy.

Figure 33. Blockchain in real estate.

The legal system is key for the future but not just regulating the uses of the technology but also as a potential sector to be disrupted. The need of third party verification for legal documents can be obsolete with the security and traceability Blockchain provides.

Security is, as we have seen in chapter 9, one of the main benefits of Blockchain technology. File keeping and data hacking avoidance are the most popular implementations of the technology in the sector.

Governments are also starting to introduce Blockchain as a technology that helps them in their performance. To foster credibility traceability of taxation through Blockchain is the biggest project of the field. However there are other projects in identification and verification of identities.

More recent business models of collaborative economies as digital rentals and ride sharing are on the focus of Blockchain technology. The differentiating value is the elimination of actual third party companies that act as trust keepers of the platform. This will mean the decrease of the commissions and therefor the price of the services.

Charities and NGO can also benefit from Blockchain. The traceability is a huge factor to create trust and involvement from donors. The problems with reputation, scandals and other misused money in the sector can be dismantled with the transparency the technology can give it.

To finish with figure 32, education system is also supposed to benefit from the technology. As happened with Healthcare sector problems with availability and traceability of academic records can be a thing of the past. With these changes human resources of companies will have access to secure and trusted transcript of applicants.

Finally, these are not the only sectors that can be disrupted by Blockchain. To put another example of a mature company that operates around Blockchain. In the sector of digital marketing, with focus on social media, IndaHash ICO raised 42 Millions of Dollars. The money served to fund the operations of marketplace that connect brands with Social media influencers as can be shown in figure 34.

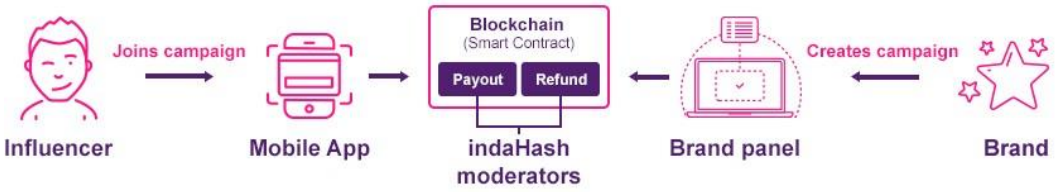


Figure 34. Indahash blockchain integration [67].

Chapter 4 A BLOCKCHAIN EXAMPLE

1. INTRODUCTION, POSSIBILITIES AND FOCUS.

As we stated in Section 2 the final idea of this research is to leverage all the previous work into showing the potential of Blockchain as a macro-economic transformation of poor countries. Aiming with these tools to reflect them, at the end, in a change of the standards of living of these populations.

In order to show the power of Blockchain we are going to plan a series of proposals that derive from a previous brainstorming and that ended in 5 final options to apply the technology. These ideas focused on access, legal security, social, International and diplomacy are presented in figure 35.

Frame	Ideas
Access	**Microcredits** to give access to land ownership to the more people as possible.
Legal security	Standardize **land registry** that agilizes and ensures the land ownerships promoting legal security
Social	**Education** to bring globalized schemes closer to local population in order to avoid conflict with foreigners.
International	**Supervision** from International Organizations and Courts to solve problems and discrepancies
Diplomacy	Bilateral **agreements** promoting investments and stablishing regulatory frames.

Figure 35. Ideas for solving the problematic.

So that the ideas proposed are all of them of a huge magnitude and all of them are valid options as they all encounter big problems that affect a lot of people. However, in order to focus the efforts we are going to have to discard four of them to stay finally with one.

Bilateral agreements between countries have been the standard practice of diplomacy and is a powerful tool but the volume of transactions and the security is not a threat and that is why not as urgent as other can be. Supervision traceability of all International Organizations standards is a complex topic that could really be benefited by the secure layer, but the cooperation needed and the mentality changes will require resources difficult to get. Education is a major theme to development

and lots of efforts are already being applied. The idea of microcredits is already been implemented with Blockchain technology in the field and that is why we will not center on it. That leaves us with registry systems maybe not the one with more hype but whose improvements can have enormous effects.

As the UN states in [68] "*the rule of law and development are strongly interrelated and mutually reinforcing*". Therefore proper regulations and legal security are key elements explaining the growth or its absence in different countries around the world. In this topic enters [69] and explains that "property rights are embedded in complex social systems". It underlines the importance of transactional costs and assures that "a general transition should take place from open access to legal or norm-based regimes with clear property rights and rules".

Land ownership security is one of the main things that need to be addressed not just to achieve development but to end lots of conflicts (see, for instance, [70]). In order to approach peace and welfare, among other important topics as access and historical rights, they need to be studied and taken into account by politicians and international organisms. But there is a clear common denominator that in words of the World Bank [71] is *"Land rights are fundamental to stimulating investment and growth"*. On the Land and Poverty Conference 2017 the organization reflected that: *"secure land rights are important for reducing poverty and boosting shared prosperity"*. Also the inequality issue affects directly this topic as *"Only 30% of the world's population has a legally registered title to their land."*.

Finally, we have set the problematic we want to solve and the idea that will lead the study of its implementation.

i EXISTING SYSTEMS

Blockchain is been implemented in some parts of the globe. Here we present some of the initiatives from we will have to learn to create a standard solution for solving this world's problematic.

India is the country where Blockchain has the most projects for land registry. The states of Andhra Pradesh [72] and Telangana [73] are preparing or partnering with startups to try land registry based on the technology. Other countries with low life conditions, Rwanda [74] and Ghana and Kenya together [75], are also entering the technology in land registry.

Developing countries are also the place for some initiatives. Ukrainian Land Registry [76] is another example. Brasil puts its confidence to save the Amazonas in land registry to end with corruption [77]. Some of this systems as the one in Georgia does not eliminate the need for governmental verification [78] but as seen in figure 36 it just leverages the technology for storage and security.

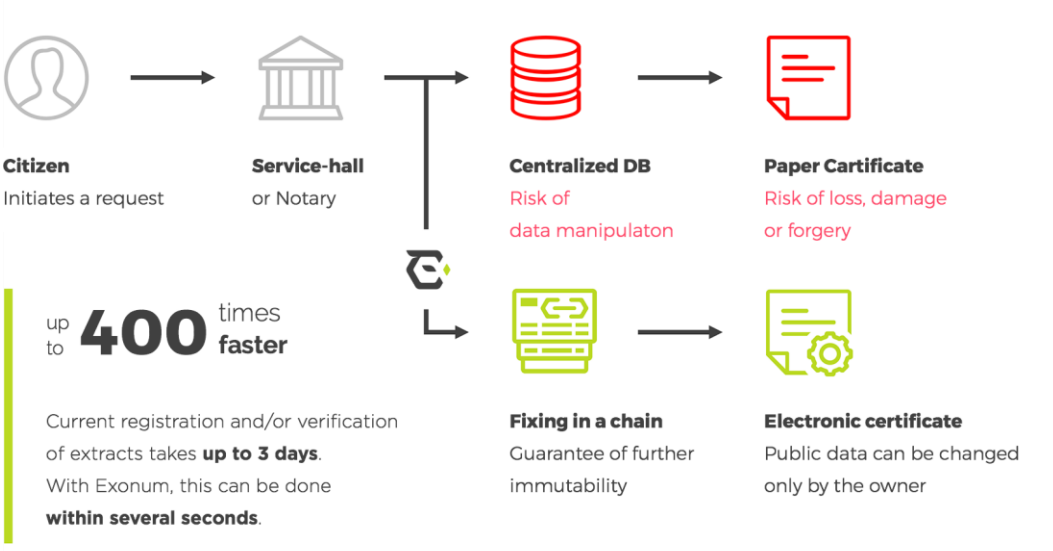


Figure 36. Georgia's Blockchain land registry functioning [78].

Developed countries are also presenting initiatives for their land registry system. Sweden [79] and Japan [80] have been the front runners in these systems. However there is no country that has yet migrated to a full Blockchain system.

2. SOLUTION PROPOSED

With the focus on the creation of a standardized, transparent and secure land registry to provide legal security and consequently growth and welfare to the countries that adopt it.

First of all, we evaluate the idea in order to clarify the features of the project. Then, we will plan the execution of it.

i EXPLANATION

Even this is not a business project, the Business canvas model [81], as presented in figure 37 but with some changes, is a good way to stablish the cornerstones of the project.

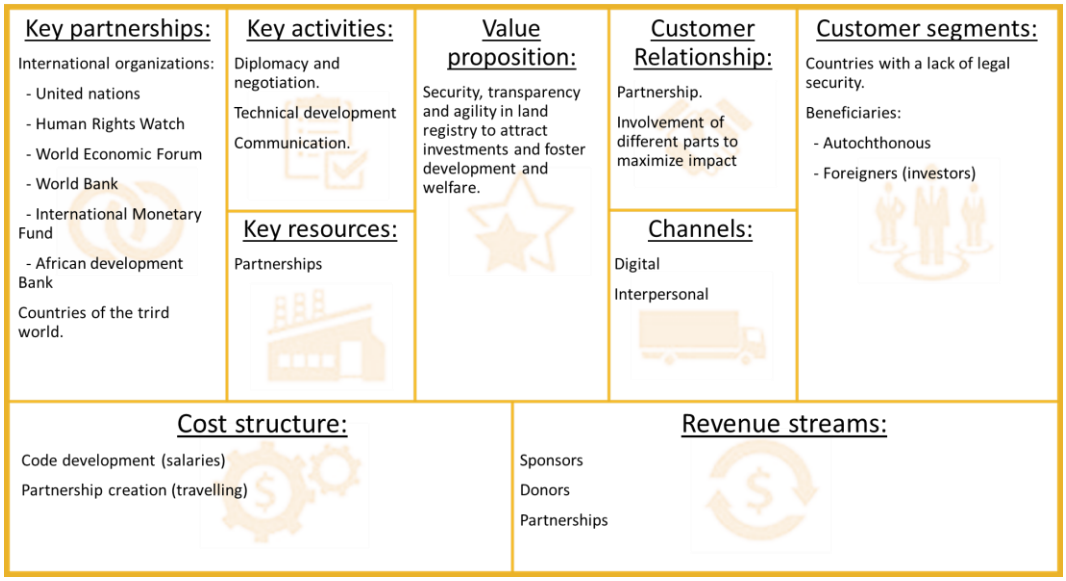


Figure 37. Business Canvas Model for solution.

To start, it is crucial for this project to get the sponsorship of partners to fulfill its purpose. This is need of, first of all, getting a channel of influence and authority to reach countries in need with the proper conditions. Also, because this project needs

the countries to bet on this project and to cooperate. In essence, the cooperation has to come in the form of resources such as money and resources to participate and maintain the network and educate and encourage their population to adopt it.

Moreover, this education is part of the key activities needed as is a big part of the communication. Diplomacy and negotiation with the different agents is as important as the technical development because if there is no partnerships the product will be doomed to failure.

As we have been highlighting our key resource is these partnerships which will have to embrace our value proposition: Security, transparency and agility in land registry to attract investments and foster development and welfare. The first part of the value proposition is the one technology holds and the other one is where communication and education takes its part. This duality is again reflected in the channels used, one digital where the product is delivered and acts and an interpersonal channel of distribution that allows the adoption and integration on the project.

Following the Business Canvas Model the part of customer relationship could well be called Partnership relationship in the aim of the project to not have customer but partners. This relationship desperately needs of the involvement the different parts because will be the countries the ones who will have to give the legal validation to the resources provided.

Our customer's main segmentation are countries with a lack of legal security or problems with digitalization and agility of their land registry systems. Also it is interesting to see that beneficiaries will be autochthonous but also foreigners as this security will make the country more suitable to foreign investments.

Finally the cost structure will be the development of the tool and the activation of partners in all its forms, as they will consequently be the ones supporting the project with the funds needed.

As we have seen it is crucial for the project to receive institutional support not just to be able to develop but also to get feedback and help from the countries and their special needs to smoother the adoption of the technology in their functioning.

As it is a product we have developed the Kotler's 4 Ps [82] which identifies the key elements in relationship place of the product in the market. The framework is summarized in figure 38 and presents the main features from the marketing mix. The product will be focused on blockchain, a single platform that allows customization through SmartContracts. The price will be free so the funding will come from donations and collaborations. The promotion will follow the international channels and the digital product is said to help low income countries.

Product	**Price**
Single. Customizable (SmartContracts) Blockchain	Free Donation and Collaborations
Promotion	**Place**
International Organization partner Personal pitching	Digital Low income countries

Figure 38. Kotler's 4Ps for solution.

The product will be a single one with no different versions but customizable due to possibility of creating SmartContracts. Such simplicity ensures security and is one of the keys of Blockchain. As we have commented, the product will be free and the structural costs of the project will be maintain with donations. The product will be promoted leveraging with relations created with International agencies and distributed digitally to low income countries trying to create a credible standard to ensure legal security.

Figure 39 shows the role of the solution as a tool that digitalizes and secures transactions of land properties between different agents. The different agents are countries and other users (people, entities, companies…). We can also observe that the product has two main layers: one for registering transactions and therefore ownership, and the other of SmartContracts that allows more sophisticated uses of the property.

First of all, with each country entering as a partner, the "transactions 0" will be done passing the responsibility of their land limits to them. As a result the register will show that the public key of the state has in its wallet all the land of its domain. After

that the existing land registry will be digitalized with transactions A. The transaction will mark the current picture of land ownership in the country.

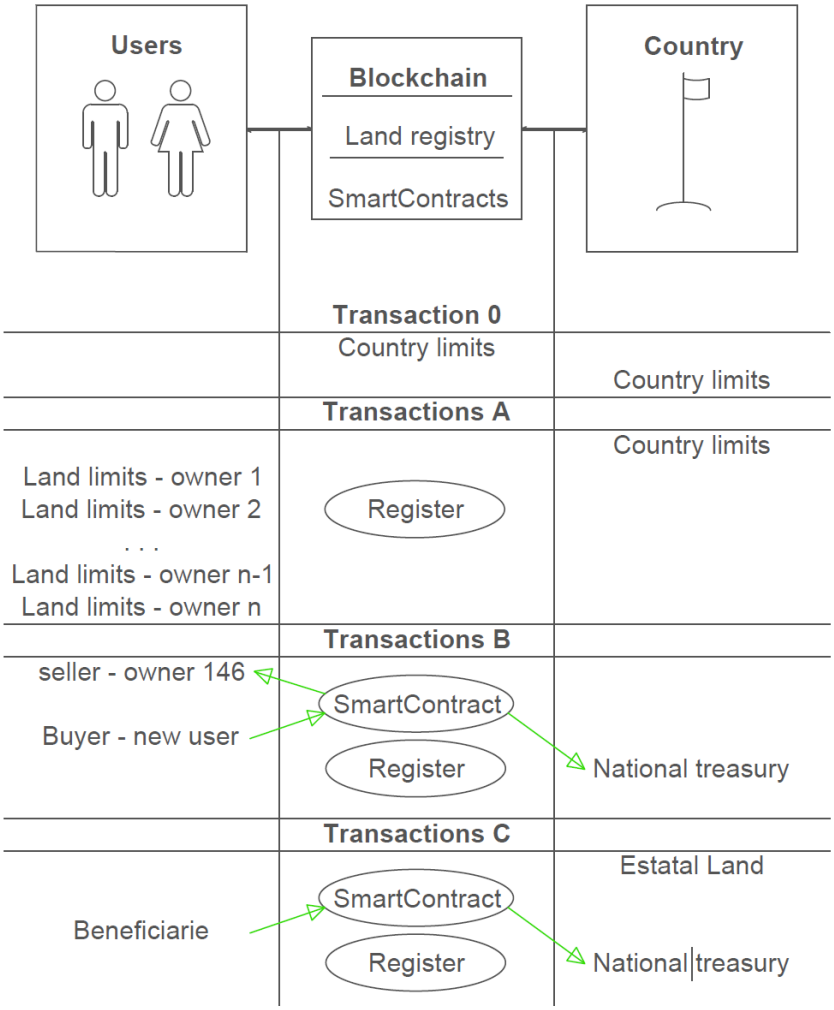


Figure 39. Diagram of type of transactions.

Once the land registry system is digitalized the software allows to stablish SmartContracts that ensures legal payments and transactions between particulars. Transactions B exemplify the sell between particulars of a land where the registration of the transaction occurs when the buyer pays the pre-established price and the money (green arrows) goes from the buyer to the seller and pays its taxes to the national treasury.

It will also allow the states to lend lands to its population and them working it end up paying to have the property. These contracts can be structure as pure lending,

lending with option of buying and sell and paying through a period of time. The specified type of actions will allow minimizing the problem of access and distribution of assets.

ii EVALUATION OF THE IDEA

Now that we have set the cornerstones of the project it is time to analyze the possibilities and main difficulties in our way. In figure 40 we have the analysis of the strengths, weaknesses, opportunities and threatens faced by the project.

	Helpful	*Harmful*
Internal	**Strengths**	**Weaknesses**
	Technological edge. The security to have a solution with low obsolescence as it is current edge. Transparency. The layer is indivisible and all movements will be hard to avoid following. Security. The cryptography under Blockchain makes it virtually impossible to modify. Agility. Reducing bureaucracy will shorten times.	Communication. It is difficult to communicate and make people engage with tools. Difficulty. These technology is difficult for non-technological users. Alignment with partners. The project needs of the partners to support and get involved.
External	**Opportunities**	**Threats**
	Interest. Land registry and legal security are key elements proved in order to prosper. Beneficiaries. The project is not directly live changing but as it affects lots of people the impact multiplies. Collaboration. Blockchain lovers that want the percepetion of the technology to change can be encourage to collaborate.	Bureaucracy. Decision making is difficult on a country and international level. Corruption. Corruption is higher in places where income is lower. Urgency. Countries where people die of hunger can feel the subject not as urgent as others.

Figure 40. SWOT for solution.

This project leverages its strengths in the ones of blockchain as shown in Chapter 9. Being able to develop a product in the technological edge gives the security of having a solution from time to come. Also Blockchain ensures security, transparency and agility.

There are also opportunities in the current landscape, this external factors can make as wind in favor for the project. The current interest from institutions for Blockchain technology and for land rights. Having a clear social mission can attract partners. Also Blockchain community can serve as most of the projects are open source and the community is very active and willing to clean the image of the technology.

Obviously there are some weaknesses that would have to be taken into account. Under all the mentioned in figure 40 there is one related with communication and acceptance of the technology. Blockchain itself does not solve the mentality changes required to implement a product of this scale. To understand better we have

adapted the framework proposed on the silent killers [83] to our project in figure 41.

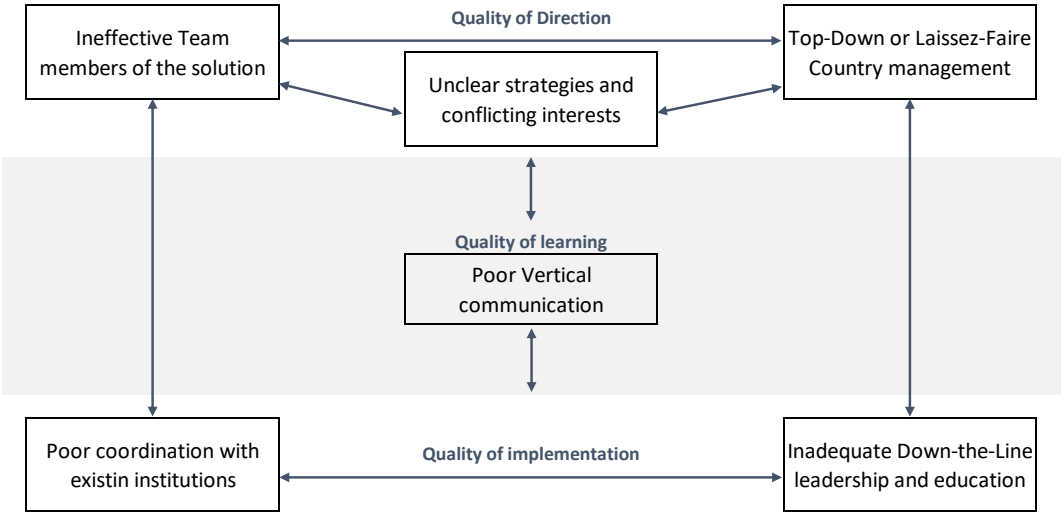


Figure 41. Silent killers for solution.

The framework provides us with three different areas of quality: direction, learning and implementation. First of all both the team of the solution and the countries' governors and managers need to set clear strategies and interests in common to direct the solution to fulfil needs.

In the middle we can find the quality of learning. All new processes suppose a change for the previous ones and in countries with low income education levels are also low [84]. Here is where communication must be effective and a lot of work under messages and different languages must be done.

Finally in the implementation coordination between different agents must be ensure to succeed. Working on materials will be key to exemplify and smoother education in the tool.

3. PLANNING

To develop the project we will try to apply as much from the methodology lean startup [85] as well as agile software development with Scrum [86]. Here we will mark the key steps to progress from an idea to a real product that can satisfy the needs demanded. This main steps are represented in figure 42

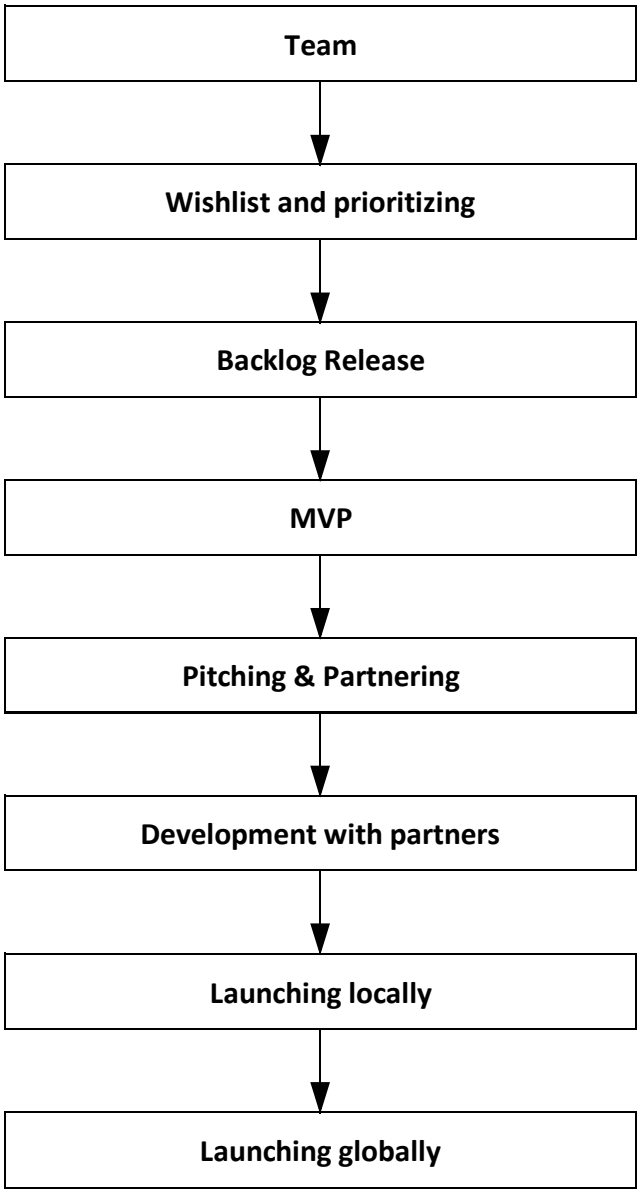


Figure 42. SWOT for solution.

The first thing will be to join a team committed and with the skills required as this is the most determinant factor in order to succeed [87]. The main skills and knowledge required are programming, third world idiosyncrasy, communication and negotiation as well as leadership.

After that we will start with Scrum methodology of creating a wishlist and prioritizing the main and basic aspects we want our minimum viable product to have. The following of the development will be done with the burndown chart as shown in Figure 43.

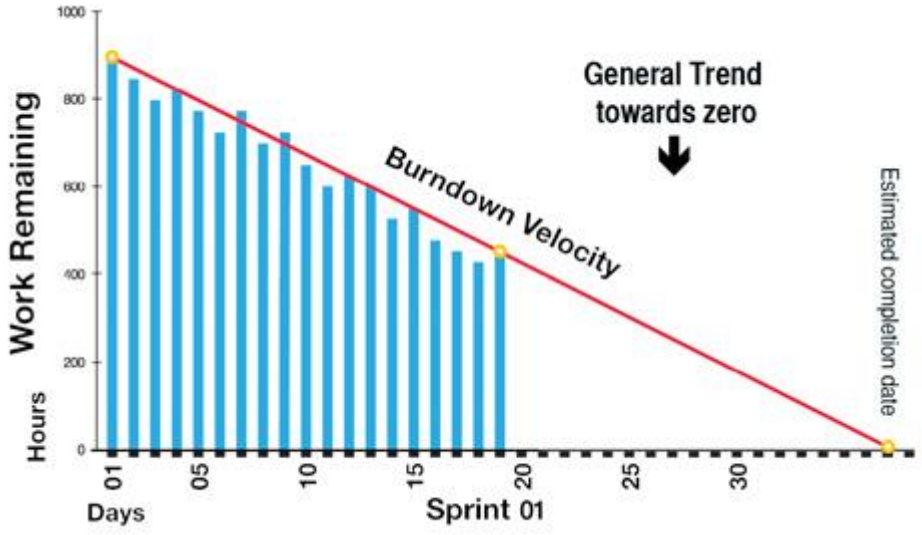


Figure 43. Burndown chart example.

With the MVP completed and ready to be shown it is time to focus on getting our key resource of partners. This will have to be done by the conventional pitching to International Organizations as the proposed on the Business canvas model that helps us getting into countries in their area of influence.

This initial partners have to be the ones testing the product and suggesting changes that prepare the product to be running in a greater scale. This way of development is called “The Provincial – Before launching world-wide, run a test on a very small sample” [88]. This way of launching provides us feedback to adjust the final features to launch globally the final product.

4. TECHNICAL SOLUTION

First of all it has to be specified what features of all are the ones we propose to develop this project. The main characteristics of the network are described in Figure 44.

name		[day/month/year]				
Public	**Permissioned**	**Consensus mechanism**				
×	✓	**Detail:**				
		PoW	**PoS**	**PoA**	**PoC**	**Social**
SmartContracts		×	✓	×	×	×
yes	**no**					
✓	×	**Protocol:** Own				
		Version:				
token	**token-less**	**Cryptographic algorithm:** SHA-3				
×	✓	**Block size:**				
		Generation time: Minutes				
name:	Local currency	**Blockchain size:**				
USD value:	Forex	**Detail:** For these type of project is better to have a more enviromental mechanism and also one that incentives partners to invest in the operation.				
Detail: Operations must be charged in local currencies						

Figure 44. Framework for solution.

First of all we have seen the problems states have with public Blockchains that is why the best alternative is to make it permissioned to make agents involved more in charge of this important information. Also the mechanism can make the registration suitable for taxation with SmartContracts. This is a feature that is not aimed in this project but is probably something important to encourage countries to adopt it. It is not tokenized because it does not want to be involved in any speculation or claims of it protecting its public mission.

Consensus mechanism must not be proof of work because even it is the most extended one is also the one with the most doubts on sustainability measurements and the project does not want to do some things better without taking into account its impact. SHA- 3 is currently the most recent standard of the National Institute of Standards and Technology of the USA for secure hashing [89]. Also the time of generation of blocks is not a key issue here as it is with financial speed.

i MINIMUM VIABLE PRODUCT

The best way to develop an MVP of a Blockchain network is to use a developing existing platform. Here the most extended and used one is Ethereum. As commented in Chapter 3 Ethereum provides a platform to create Blockchain initiatives and provides a great community and resources for learning.

In all the development we want to work with agile methodologies. For the software development the Scrum methodology will serve as a guideline. The workflow is presented in the framework of figure 45.

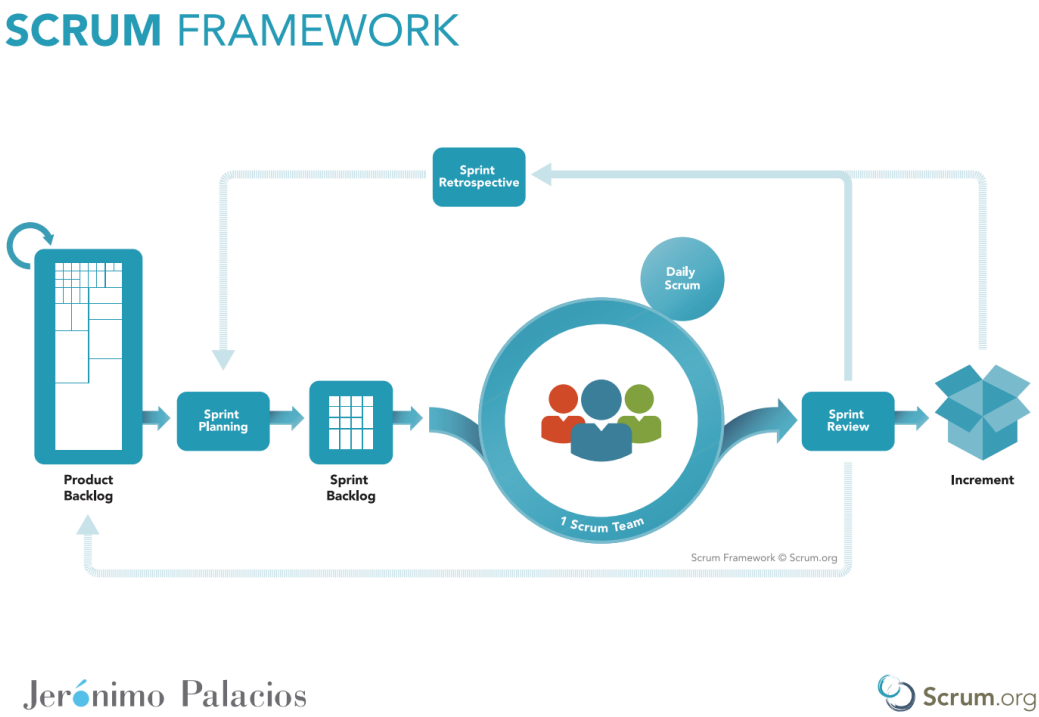


Figure 45. Scrum framework [90].

Before, we are going to create a wish-list were we want to specify the desired main features for the MVP network. This wish-list is going to be prepared thinking on the constraints of this prototyping. This whishes are the minimum features desired to have to be able to show the usability and functioning of the idea. The summary of this features is showed in figure 46.

Figure 46. Wishlist for solution.

In the figure, we can observe that this are the minimal things to do to start presenting the proposal and its functionalities to test the real interest on it. With all this information it is time to get more concrete, prioritize and adjust to the Ethereum network that is going to be used. Finally we will have to create a Product backlog for the MVP. The backlog is presented in figure 47.

Main	Explanation	Estimation
Ethereum Blockchain		92
	Prepare network features	55
	Create manager user	3
	Set documents properties	13
	Create network constraints	21
Web page home		81
	Draft	21
	Decide framework	5
	Code	55
Web page user profile		29
	Decide member creation way	8
	Implement web membership	21
Web page user profile		29
	Create template	8
	Integrate google maps	21
Back-end		47
	Data storage	13
	Data processing	34
Integration		42
	Communications	34
	Contingencies	8

Figure 47. Backlog for MVP.

In figure 47, we have divided the wish list in smaller tasks in order to adjust as much as possible in the estimation of times for each task. In the estimation of times, we have followed the use of the Fibonacci sequence as it is a great way to avoid the uncertainty of dealing with the estimation of big times [91].

First of all, to create the Ethereum Blockchain we will have to prepare the different features for the integration in the platform. This part is the key and it represent a huge part of the process. To be able to interact with Ethereum we will need to have our own user to have an account. The documents the platform will kept the record off have to be stablished. Finally, the constraints have to be set and clarify to success in a rational functioning.

The front end development is key not just for functioning but for marketing also. This has to be not just a coding task but also a design one. The process will be first, defining what the home page wants to say and do in a draft. After that, the proper framework for developing has to be selected according to the features specified in the draft. At the end, coding in the framework will gave us our first view of the home page.

The following two wishes stablish tasks that are continuing with the same abilities previously used. Key plugins as google maps for viewing and managing mapping information must be addressed. We have selected Google as it is the most popular map provider and it is free.

The back-end must gear that transmit information from Ethereum to the users and vice versa. That is why, data storage must be addressed and structuring is a key task to ensure a correct functioning. The better the structure is the lesser complications will be with processing.

Finally, the integration of all parts is the last assembly for the project to start running. Here communications play a central role, as protocol definitions and server managing will limit the quantity of usage the network can support. With all this in mind the planning of contingencies is also a required task in order to avoid future problems.

Also in figure 48 we can see that tasks have been organized in sprints to align with the process described in figure 47. These sprints have been thought to be small MVPs inside the whole development. For that we will leave margins to follow the process of plan, do and check to ensure always doing the work correctly.

Main	Explanation	Estimation
Planning sprint 1		13
Ethereum Blockchain		92
	Prepare network features	55
	Create manager user	3
	Set documents properties	13
	Create network constraints	21
Testing		13
Sprint 1 total		**118**
Planning sprint 2		13
Web page home		81
	Draft	21
	Decide framework	5
	Code	55
Testing		5
Sprint 2 total		**99**
Planning sprint 3		13
Web page user profile		29
	Decide member creation way	8
	Implement web membership	21
Web page user profile		29
	Create template	8
	Integrate google maps	21
Testing		8
Sprint 3 total		**79**
Planning sprint 4		34
Back-end		47
	Data storage	13
	Data processing	34
Integration		42
	Communications	34
	Contingencies	8
Testing		21
Sprint 4 total		**144**

Figure 48. Sprints for MVP.

The sprints presented in figure 48 have been planned to be able to test different steps to minimize the accumulation of the errors in the end. The total amount of hours needed to fulfill the project result on 440.

The structure of the resulting MVP is shown in figure 49. From one side we will have the users that interact with the front-end, and from the other we have the Ethereum platform. Through the Application programming interface we interact with the network. The back-end acts as the moderator of the two sides managing data to ensure an optimal process of the information.

Figure 49. Schema for technical MVP.

Chapter 5 FUTURE DEVELOPMENTS

From the first part, the technology is still developing. That is why this document will need updates in future to adjust to new trends and features as well as changes in the algorithms, cryptography, typologies and new mechanisms to reach consensus in the network. Further revisions of the framework will be needed to maintain its ability to highlight the main boundaries of each alternative.

The second part outlines the main current uses of Blockchain. Apart from updating to changes in its uses, there is plenty of work to be done analyzing more in depth each sector potential disruptions. Also, the estate of maturity of the technology alerts that small initiatives that now can be out of the radar from the public can be important players in the not too distant future.

Finally, the last part can serve as a start to an electronical master thesis on the coding and development of the solution proposed. The problematic is not an easy one and any other development to reduce its effect will be extremely useful. Most of the planning here proposed can be developed with a technological background on coding. The choosing of Ethereum should serve as encouragement to further developments. This platform has a lot of resources to learn, the community is very active and is thought to be an easy way to introduce new adopters to the technology.

Chapter 6 CONCLUSIONS

The Project has three different parts that left us with a common conclusion: Blockchain technology is currently not a mature enough technology to conclude its impact but enough to asseverate that it is here to stay and its possibilities are immense.

From the first part, we can conclude that Blockchain is been a technology developed differently to what we were used to. Instead of being created in a university or the R&D department of a company, it was originate from a person or group whose identity has not been leaked out. This issue has marked it setting it aside from canonical standardization. However, the framework created serve to create a visual tool that condense much of the information needed to differentiate the different technical variants of the technology.

Studying its current uses we confirm that it is an active technology not yet settle. Most industries are trying to be prepared to the disruptive potential of the Blockchain. Financial industries are the ones more concerned with it. Nevertheless, as has been shown most industries are starting to see projects with this knowledge enter their sectors. Also, there are initiatives that try to bring closer the technology to the public, being Ethereum the most relevant platform to develop projects with Blockchain.

Finally, Blockchain benefits translate perfectly to solve problematics with third party trust. This has been focus to solve the problem of land registration in third world countries. This countries have lots of problems (and possibilities) but in the current globalized world property rights and legal security are key to attract investments and therefore growth and prosperity. Security and traceability are the key benefits of this particular technology that makes it perfect to tackle the problematic avoiding the need of a third party to trust the maintenance and validation. Also, Blockchain does not needs of a special way of managing its project and frames itself perfectly in software development framework as Scrum.

BIBLIOGRAPHY

[1] Don Tapscott and Alex Tapscott. BLOCKCHAIN REVOLUTION: How the Technology Behind Bitcoin is Changing Money, Business, and the World.

[2] http://www.undp.org/content/undp/en/home/blog/2018/realizing-the-potential-of-blockchain-for-social-impact.html

[3] https://nairobi.worldblockchainsummit.com/

[4] https://blockchainforsocialimpact.com/

[5] https://ethichub.com/

[6] https://www.forbes.com/sites/davidhessekiel/2018/04/03/the-future-of-social-impact-is-blockchain/#177c7ab9c3fd

[7] https://www.forbes.com/sites/stevedenning/2017/11/30/why-the-world-is-getting-better-why-hardly-anyone-knows-it/#15e087a07826

[8] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

[9] PwC- http://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/qa-what-is-blockchain.pdf

[10] Christopher Cannucciari. 2016. Banking on Bitcoin [Documental]. EEUU: Netflix

[11] https://www.activism.net/cypherpunk/manifesto.html

[12] https://www.marketwatch.com/story/wikileaks-founder-julian-assange-bitcoin-is-the-real-occupy-wall-street-2017-12-15

[13] https://blockgeeks.com/wp-content/uploads/2017/08/image5.png

[14] Rafael Pass and Elaine Shi. Hybrid Consensus: Efficient Consensus in the Permissionless Model. Retrieved from: http://drops.dagstuhl.de/opus/volltexte/2017/8004/pdf/LIPIcs-DISC-2017-39.pdf

[15] https://hardwareate.com/prueba-de-trabajo-vs-prueba-de-participacion

[16] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Proof of activity: Extending bitcoin's proof of work via proof of stake

[17] https://minergate.com/blog/why-proof-of-capacity-could-be-the-future-of-cryptocurrency/

[18] Boroujerdi and Wolf. Goldman Sachs. Emerging Theme Radar. What if I told you… Equity | December 2, 2015

[19] Bank of America Merril Lynch. Global Technology. Blockchain: exploring the potential. Equity | 31 May 2016

[20] What is blockchain? - Business Insider. www.businessinsider.com

[21] Karan Bharadwaj. Blockchain 2.0: Smart Contracts. August 7, 2016

[22] Allison, Ian. "PwC blockchain expert pinpoints sources of ambiguity in smart contracts". 12 August 2016. IBTimes (News). Retrieved from: https://www.ibtimes.co.uk/pwc-blockchain-expert-pinpoints-sources-ambiguity-smart-contracts-1575778

[23] http://www.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1?IR=T

[24] Jiasun Li & William Mann. Initial Coin Offering and Platform Building. April 2, 2018.

[25] https://towardsdatascience.com/blockchain-technology-explained-to-your-grandma-bfea5ba876ac

[26] F. Xavier Olleros and Majlinda Zhegu. Reasearch handbook on digital transformations. Chapter 11, page 225.

[27] https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462

[28] https://techcrunch.com/2018/01/28/bank-based-blockchain-projects-are-going-to-transform-the-financial-services-industry/?guccounter=1

[29] https://www.oreilly.com/ideas/understanding-the-blockchain

[30] https://www.forbes.com/sites/dantedisparte/2018/11/12/to-blockchain-or-not-to-blockchain/#4d0ef05373cb

[31] Oliver Wyman and J.P. Morgan. Unlocking Economic Advantage with Blockchain. A guide for asset managers.

[32] Saveen A. Abeyratne and Radmehr P. Monfared. BLOCKCHAIN READY MANUFACTURING SUPPLY CHAIN USING DISTRIBUTED LEDGER. International Journal of Research in Engineering and Technology.

[33] Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles. A Blockchain-Based Approach to Health Information Exchange Networks. Mayo Clinic.

[34] Matthias Mettler. Blockchain technology in healthcare: The revolution starts here. Boydak Strategy Consulting AG, Freienbach, Switzerland

[35] https://www.adp.com/spark/articles/2018/03/transaction-technology-hr-and-the-blockchain-benefit.aspx

[36] Monsalve, Salcedo and Albeiro. Blockchain: 3.0 the Technological Solution to Face Corruption. Contemporary Engineering Sciences, Vol. 10, 2017, no. 34, 1651 – 1658

[37] https://cartorios.org/wp-content/uploads/2016/06/2016-06-26-sweden-tests-blockchain-technology-for-land-registry.pdf

[38] https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

[39] http://blockchaincommission.org/

[40] https://www.investopedia.com/terms/h/hard-fork.asp

[41] https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/

[42] https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/

[43] https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/

[44] http://uk.businessinsider.com/bitcoin-mining-electricity-usage-2017-11?IR=T

[45] https://www.cnbc.com/2017/12/21/no-bitcoin-is-likely-not-going-to-consume-all-the-worlds-energy-in-2020.html

[46] https://www.investopedia.com/terms/c/cryptocurrency.asp

[47] http://www.visualcapitalist.com/interactive-ranking-20-cryptocurrencies/

[48] https://en.bitcoin.it/wiki/Protocol_documentation

[49] https://www.coindesk.com/price/

[50] https://www.express.co.uk/news/world/872831/catalonia-spain-news-independence-new-cryptocurrency-estonia-defy-eu

[51] https://ripple.com/

[52] https://ripple.com/build/xrp-ledger-consensus-process/

[53] https://www.forbes.com/sites/quora/2018/02/08/what-is-litecoin/#2c3ff07533f7

[54] https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance

[55] https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/

[56] DR. GAVIN WOOD. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. EIP-150 REVISION (759dccd - 2017-08-07)

[57] https://github.com/DavidJohnstonCEO/DecentralizedApplications

[58] Allen & Overy. Decentralized Autonomous Organizations. Retrieved from: http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralized%20Autonomous%20Organizations.pdf

[59] https://blockchainhub.net/dao-decentralized-autonomous-organization/

[60] PwC global power & utilities. Blockchain – an opportunity for energy producers and consumers?

[61] EY. Overview of blockchain for energy and commodity trading. Retrieved from: http://www.ey.com/Publication/vwLUAssets/ey-overview-of-blockchain-for-energy-and-commodity-trading/$File/ey-overview-of-blockchain-for-energy-and-commodity-trading.pdf

[62] World Energy Council in collaboration with PricewaterhouseCoopers. The Developing Role of Blockchain. White paper.

[63] https://www.indigoadvisorygroup.com/blockchain

[64] https://www.forbes.com/sites/bernardmarr/2018/07/16/here-are-10-industries-blockchain-is-likely-to-disrupt/#67286108b5a2

[65] https://www.democracy.earth/

[66] https://www.forbes.com/sites/stevedenning/2017/11/30/why-the-world-is-getting-better-why-hardly-anyone-knows-it/#15e087a07826

[67] https://medium.com/@indahash/indahash-blockchain-based-campaigns-revolution-aca028c1d52f

[68] https://www.un.org/ruleoflaw/rule-of-law-and-development/

[69] Daniel Fitzpatrick. Evolution and Chaos in Property Rights Systems: The Third World Tragedy of Contested Access. The Yale Law Journal. Volume: 115. Number: 5. March 2006.

[70] Inequality and Social Conflict Over Land in Africa. Pauline E. Peters. Journal of Agrarian Change, Vol. 4 No. 3, July 2004, pp. 269–314.

[71] http://www.worldbank.org/en/news/feature/2017/03/24/why-secure-land-rights-matter

[72] https://www.coindesk.com/andhra-pradesh-partners-with-chromaway-to-develop-blockchain-land-registry

[73] https://economictimes.indiatimes.com/small-biz/security-tech/technology/blockchain-tech-is-joining-e-gov-dots-in-ap-telangana/articleshow/59330625.cms

[74] http://isiafrica.net/rwanda-to-adopt-blockchain-technology-for-its-land-registry/

[75] https://africabusinesscommunities.com/news/africa%E2%80%99s-first-multinational-blockchain-land-registry-to-be-launched-in-kenya-and-ghana/

[76] https://www.bloomberg.com/news/articles/2017-10-03/ukraine-turns-to-blockchain-to-boost-land-ownership-transparency

[77] https://www.reuters.com/article/us-brazil-property-blockchain/can-blockchain-save-the-amazon-in-corruption-mired-brazil-idUSKBN1FE113

[78] https://exonum.com/napr

[79] https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain

[80] https://bitsonline.com/real-estate-zweispace-japan-blockchain/

[81] Alexander Osterwalder & Yves Pigneur. Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. July 2010.

[82] Kotler, P., Marketing Management, (Millennium Edition), Custom Edition for University of Phoenix, Prentice Hall, 2000, p. 9.

[83] Michael beer and Russell A. Einstat. The silent killers of strategy implementation and learning. Sloan Management Review; Summer 2000; 41, 4; ABI/INFORM Global. pg. 29

[84] Eric A. Hanushek & Ludger Wößmann. Education Quality and Economic Growth. The World Bank. Retrieved from: http://siteresources.worldbank.org/EDUCATION/Resources/278200-1099079877269/547664-1099079934475/Edu_Quality_Economic_Growth.pdf

[85] Eric Ries. The Lean Startup.

[86] Jeff Sutherland. Scrum: the art of doing twice the work in half the time.

[87] Alex Charfen. The Most Important Success Factor in Your Business. Retrieved from: https://www.huffingtonpost.com/alex-charfen/the-most-important-succes_1_b_5790488.html

[88] Alberto Savoia. Pretotype It: Make sure you are building the right it before you build it right. Second Pretotype Edition. October 2011.

[89] https://www.nist.gov/publications/secure-hash-standard

[90] https://jeronimopalacios.com/scrum/

[91] Mike Cohn. "Agile Estimating and Planning". Mountain Goat Software. November 2005

Parte II ESTUDIO

ECONÓMICO

Chapter 7 ECONOMICAL STUDY

In this chapter we present a briefing of the costs that need to be satisfy to have a minimum viable product. This costs will cover from the MVP to start presenting it to future partners.

The first assumption that we need to do is how much time we are willing to invest to develop the MVP. For it to make sense, it has to be lesser than programming hours needed that we obtained in chapter Chapter 4 section 4. Viewing the needs of the project 3 persons will be needed to success. The main cost assumptions are: legal support and office renting, whose value has been estimated from asking entrepreneurs; salaries whose value is the salary (minimum planned by national government) plus a 35% more from the real cost for a company; Partner capitation has been guessed from the cost of travelling to a European capital two persons for two days; hosting has been assumed from domain buying plus hosting prices from the internet; and Gsuit is the cloud service and mail provider of google.

	Total	Total hours available	Programming hours
Months	3	504	440

Workers	Number
Total	3
Programming	1
Marketing	1
Direction	1

Assumptions	Cost/month
Legal support	300
Office renting	700
Salaries per worker	1215
Partner captation	600
Hosting	22
Ethereum expenses	8
Gsuit per user	4

Costs	Monthly	Total	Percentage
Office	700	2100	13%
Central	300	900	6%
Salaries	3645	10935	69%
Technology	42	126	1%
Marketing	600	1800	11%
Total	**5287**	**15861**	**1**

With this costs we can observe that the most important item are salaries followed by the renting a space to work.