# Blockchain

## How to develop trust in complex surroundings to generate social impact value.


**ITE/IPS TechLab**

**Author: Marcos Allende López**

**Illustrations: Vanessa Colina Unda**


IDB

## INDEX OF CONTENT

This document is the result of the work conducted in ITE/IPS, led by Marcelo da Silva, to present blockchain technology from a technical and practical point of view, with the intention of it being useful for the Bank's specialists in the various fields where it can be applied. It would not have been possible without the involvement of Raul Cerrato in the technical investigation, the strategic vision of Marina Gutierrez Aldabalde and the design and illustrations by Vanessa Colina Unda.

This document is divided into three content blocks, the conclusions and an annex. The first block consists of a brief presentation of the technology; the second block tackles the technical aspects of the same, not in an excessively formal sense but rigorous and the third block talks about the matters most related to the convenience, application and utility of blockchain for specific projects, with a checklist and a detailed use case. The annex briefly presents the cryptocurrency field.



## Introduction

Since Bitcoin adopted blockchain technology in 2008, the interest in it has increased in an exponential manner. Even if its first and most successful use has been cryptocurrency, there is a great global and multidisciplinary interest in its potential to offer large-scale solutions in various fields.

This document aims to be a fast guide in understanding how blockchain technology Works, what are the characteristics that make it different and revolutionary and what are the cases for which its implementation is beneficial.

It also presents the differences between types of blockchain, tackling the questions that one must ask to determine if one is convenient, and in case it is, which as a tool could build a solution that would be useful for a determined project.

# Birth and evolution of blockchain technology

The first publication[1] about blockchain technology dates back to 1991. The authors' idea consisted in having a digital ledger of archives, audio, images, video or text, chronologically ordered, which would permit an exact understanding of its creation and authored date.

Almost two decades later, in 2008, Bitcoi[2] is born. The proposal of this cryptocurrency consists in using blockchain technology to provide an electronic method of payment that does not need supervision and eludes control of financial institutions. The fundamental and defining ingredient that incorporates Bitcoin making it, to date, the most successful digital currency proposal, is the combination of the intelligent idea of blockchain technology along with a consensus protocol known as **Proof-of-Work**. As we will explain later on, this is the mechanism through which the cryptocurrency transactions are validated, proving, for example, that the money transferred exists and has not yet been spent, and the validators are rewarded with a certain quantity of virtual money. In the wake of its success, others have followed in its steps making the number of cryptocurrencies in circulation to date exceed that of 2000.

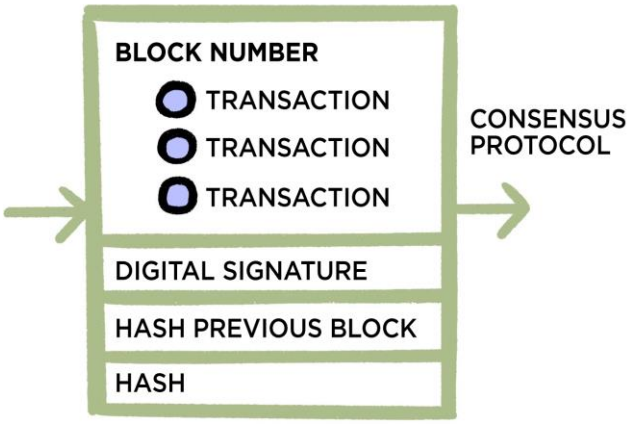
Regarding its application outside of the cryptocurrency world, of which this document will focus on, its use as a tool with multiple applications in very diverse fields has been in study and exploration since 2008. Some of the most attractive uses are the decentralized ledger of documents, medical histories, property ledgers, organization and distribution of energy resources, border control, voting systems, digital identity or monitoring of production processes.

[1] **S. Habber, W.S. Stornetta – *How to time-stamp a digital document,* 1991.**
[2] **Sathosi Nakamoto – *A Peer-to-Peer Electronic Cash System,* 2008.**

# What is blockchain?

In general terms, blockchain is a ledger of distributed[3] information such as **P2P (Peer-to-Peer)** in which the different participants **do not need to trust each other**. Instead, the **consensus protocol** put in place guarantees the security and veracity of the transactions. Another of its main characteristics, and without a doubt one of its most relevant, is the **immutability of the chain**; in blockchain it is impossible to edit or erase information.

The term blockchain is due to the structure of the ledger, consisting of groups of transactions, which are organized and stocked in blocks. The blocks are **ordered chronologically** and have a **block number**, an alphanumeric code such as **hash**, of which we will go into more detail later on and are **digitally signed** by the person that proposes or validates the block.




From the inverse perspective, the blocks can be seen as groups of transactions that have been assigned a block number and a hash code. Regarding the immutability of the chain, in the case that introduced information in a validated block wants to be changed, the only way to do so would be issuing a new transaction that updates the desired information. **It is in no way possible to edit or erase** anything that has been previously validated and added to the chain.

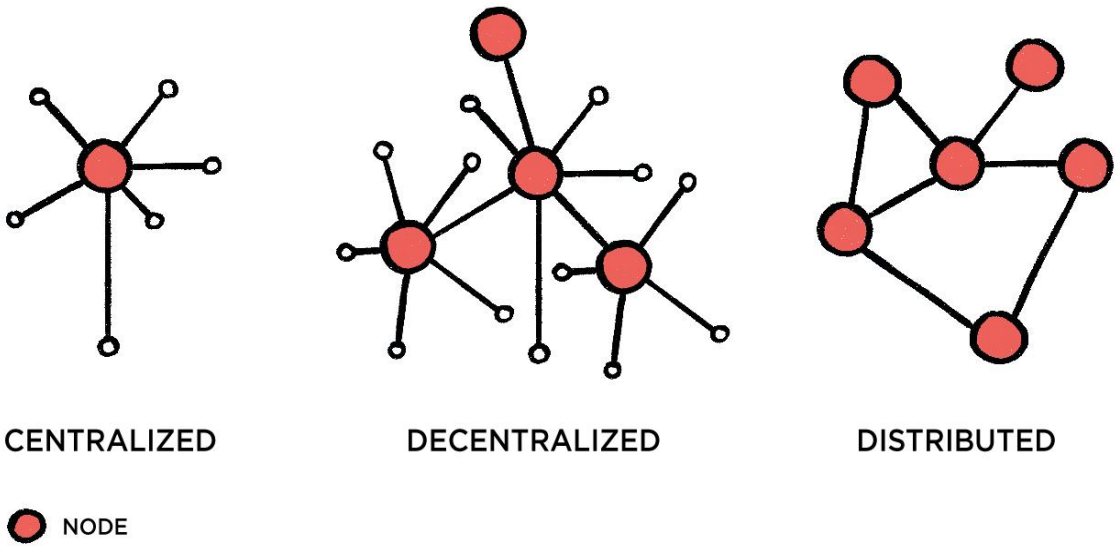
[3] **Even though it could be defined as such, blockchain is not a database given that its main purpose is not to store data but to register transactions. In fact, as we will discuss further on, we often need a database to complement the blockchain to store heavy documents, due to efficiency reasons. Otherwise, the blockchain copies that each authorized participant possesses would become too heavy.**

## a. Distributed ledgers

The databases or ledgers of centralized information can be defined as such where facts are stored in a unique physical place, a unique server, even if it is accessible from other places and by different entities. In contrast, the decentralized and distributed databases are stored in various servers.

**Blockchain is born as a distributed information ledger proposal**, and operates in such a way that each of the computers or servers connected to the ledger has a **copy of the whole blockchain**.

It is not just a matter of where the information is stored, but also of who is in charge of it, because in blockchain, not only do all of the participants have a copy of the blockchain but also all are in the **same hierarchical position** regarding decision-making, proposition and block validation. This completely eludes the necessity of a central entity. Not one of the participants can impose over the other, even to the point of not being able to add new information without the consensus and authorization of the rest.



## b. P2P (*Peer-to-Peer*)

P2P refers to the fact that interaction between different participants, which we will call **nodes**[4] from now on, is done by pairs. The nodes are not all connected with each other, but **each node is only connected to a determined number of the rest**. The value in this can be seen in terms of efficiency and anonymity, such as is explained in page 43. When a node wants to make a transaction, it sends this information to its connected nodes and those replicate that with their own. The process continues until the information is shared with the whole network. This occurs like so, unless the sent transaction is invalid, for example, if someone tries to send non-existent money, in which case when the nodes "listen" they simply ignore.

## c. No need to trust

In traditional databases it is assumed that all the participants are trustworthy, so to say, that none of the nodes, in the language we are using, are going to introduce false information to the database. The revolutionary idea of blockchain consists in offering a consensus protocol that permits no need for trust between nodes and therefore allows for them to share a ledger of sensitive information. The consensus protocol serves **to avoid the addition of blocks with false information to the chain** or, if they are unlikely added, to be rejected by the rest of the nodes.

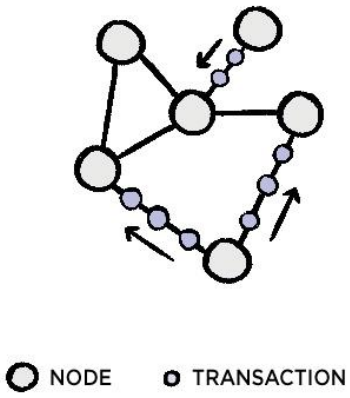
**[4] The term node is used in database language to refer to the physical server where the information is stored. In blockchain language, this term is used to refer to the person or participant that is connected to the blockchain and using the node server, given that in the public networks, of which we will discuss later on, all of the participants, will interact as nodes with the network. In the private and federated networks it is necessary to be more precise and explicit when defining the concepts of node and participant.**

## How blockchain technology works?

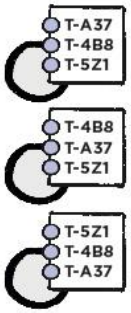
The process through which information is generated and new valid blocks are published can be described in the next six steps. It is convenient to clarify that the meaning of the word **transaction**, in this context, **encompasses any type of information exchange susceptible of being contained in a block**. Information about a financial transaction, a smart contract, a change in the user permissions -in the case that the network permits such a possibility- and a long etcetera. In general, any information that has to do with blockchain, be it in relation to its participants or to the information that they share, is registered in a block of the blockchain in the form of a transaction.

**Step 0**. Any person or collective of people that want to be part of the network have two options in function of the type of blockchain that is being used; **downloading the corresponding application** that converts them in a node with the same rights as the rest, or **accessing via a web interface** that the administrative nodes had provided for the rest of the authorized users. The first option generally corresponds to public networks, where whoever wishes to participate, only needs to download the corresponding software and, in an automatic way, connects with a determined number of nodes and asks them for the most updated copy of the blockchain. The alternative option corresponds to federated or private blockchains, of which we will talk more soon. In these blockchains there will be some privileged nodes administering the chain and deciding how the "regular user" accesses through a web interface that they will provide.

Step 1. Once the participants are connected to the chain, the first step consists of sending the information in the form of transactions that will finally end up constituting the blocks. So to say, when a node wants to make a transaction, be it a financial operation, a Smart Contract, etc., **it sends the information of this transaction to the nodes with which it is connected**. Here, a first protocol automatically takes action in that **each node proves that the "heard" transactions are valid**[5], for example, that spent money is not trying to be transferred. In the case that the transaction is correct, **each node adds it to its list of transaction**, which we will now call by its contextual name: **pool**, and resends it to its connected nodes. The process continues but not forever since, when one node receives information about a transaction that is already in its list or pool, it simply ignores it.



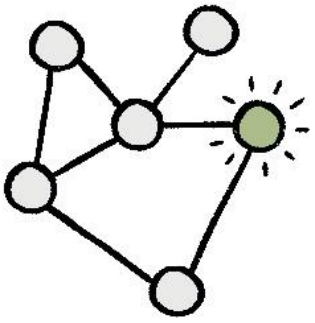

[5] **Due to the fact that the concept of transaction encompasses any type of information added to the network and that each network has its won architecture, the way in which it is determined if a transaction is valid or not depends on each particular case. An example are the automatic processes that occur, for example, when financial transactions are made in which it is proven that the sender has the sufficient funds. Another example are the not automatic processes in which specific participants of the network, generally in federated or private networks, validate, for example, that a shipment arrived to port, that the size of a shipment does not exceed the requirement or emit a certificate.**




NODE TRANSACTION

depending on the blockchain, takes place in a time frame that can last on average from a few seconds to several minutes, a node is **randomly chosen to propose a block**. This process is the most important, since it is the one that makes the blockchain a ledger in which the distinct entities don't have to trust one another. The way in which the node is randomly chosen is known as the consensus protocol and it will be explained in the next section. The

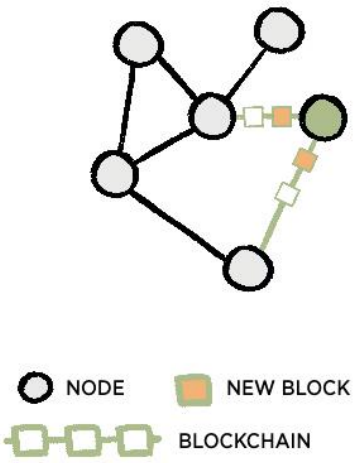
Step 2**. Each node fills its list or pool** with the transactions it hears. In general, the pools of two different nodes don't have to coincide since the norm is that they hear transactions in a different order.

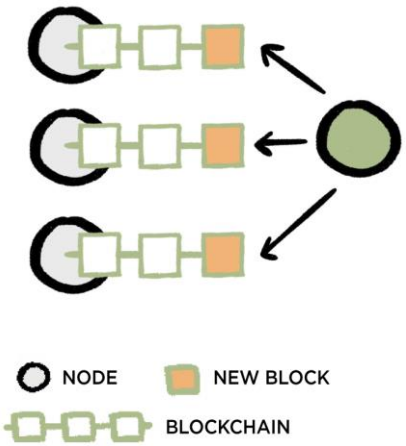


NODE SELECTED NODE

way in which the chosen node proposes the block is by taking the updated version of the chain, adding a block at the end that contains the transactions it had been adding to its *pool* and sending this new copy of the chain to its connected nodes, who will replicate this to the rest of the network just as they did with the individual transactions. The blocks have a maximum size that depends on the blockchain, which is why they fill up with a limited number of transactions.

Step 4**. The chosen person proposes a new block with the transactions that it has been "hearing" and registering in its pool**. Before being sent to the rest of the nodes this block must be validated with a **hash**, which is the alphanumeric code obtained from the block information. In the next section we will talk in detail of how this code is found, who makes it and what it is for.






Step 5. The system, the internal protocols of the blockchain, only accepts the block if it has a valid hash. In a positive case, the rest of the **nodes verify** that all the transactions are also correct **and update their copy of the chain** with this new version that contains the new block.

## Consensus protocols

The consensus protocol is the **process during which a node is chosen to propose a new block**. This selection is random, such as was discussed in the previous section, even though not all the participants have the same probability of winning the "raffle".

The purpose of the random election is **to avoid there be a sole person responsible for the proposal of blocks** that could take ownership, in this way, of the chain. For that, it is desired that all the participants can be chosen to propose blocks but those who have a greater individual interest in the correct development of the blockchain have a higher chance of winning the raffle.

Mainly, there are two forms of determining this interest. The first is **to demand the people or entities to make an effort to compete to be the chosen and give a reward to the winner,** usually, in the form of cryptocurrency. The second is to **distribute the probabilities of winning the raffle proportionally to the number of assets, properties or goods in the network of each participant**. Let's see some examples.

Proof-of-Work (PoW)**.** PoW corresponds to the group of consensus protocols where **an effort is demanded from the participants in order to win the raffle and propose the next block, and the winner is given a reward.** The effort consists of **using computational capacity to find the hash code**, which validates the last block. In the next section we will talk of how it is obtained, but for the moment it is enough to know that a computer does random trials to find it. The more capacity the computer has, the greater the energy consumption and the higher the probability of obtaining the valid code.

What happens is that when someone proposes a new block, they do it without a hash code, so **that all the nodes can compete to find it**. Only some do this and they are known as miners, due to the fact that **the process of finding a hash is known as mining.**

Given that employing computational capacity to find the hash implicates spending money, and that no node has the guarantee of being the first in finding it, it seems unreasonable that a malignant node would spend its energy and money in this purpose. Even more so keeping in mind that, if it wins the raffle and proposes an invalid block, the rest of the nodes would reject it and it would not receive the reward.

To motivate the non-malignant miners in trying to find the valid hashes, the blockchains that implement this method offer a reward in the form of cryptocurrency to the first node that finds it. To date[6], the reward for each valid block in Bitcoin is 12.5 bitcoins, which translates into more than $185,000 dollars, and one block is validated, on average, every 10 minutes. This method can only be used in blockchains associated to cryptocurrencies.

One of the arguments wielded against this protocol is the **high amount of energy employed**, some would say wasted, in validating or mining blocks. On one hand, it is necessary to say that this process doesn't just work to determine who proposes the next block but it also redounds in the security of the chain. As we will see in the next section, if someone modifies something in the block, that block along with the ones after it, will have an invalid hash, which would need to be mined again.

So to say, if someone were to modify the blockchain it would have to mine not only that block, but also all of the ones before it, again. And it would have to do so in each copy of the blockchain, which is in each node's property. As it is evident, the difficulty that said hacker would have to overcome would be the same one as the initial miners. Closing the argument, the person who wishes to corrupt the network would have to spend as much energy as it did in validating it originally. If difficulty is high, the employed energy is higher but so is the security.

[6] **To the day, January 9, 2018.**

The reason why, despite that, all of this energy is spent is that **the difficulty of the hash is not configured in function of how much security it aims to have but of the average time it takes to mine**. So to say, because the miners compete in finding the hash for each block, if the mining difficulty was fixed based on having enough security for the chain, then when the miners increased in number or in their resources, the blocks would be mined faster each time and would therefore be more empty -containing less transactions-, meaning they would have less transactions. This interests us, so that what is fixed is the average time it is desired for the blocks to take in being mined. In Bitcoin it is 10 minutes, and approximately every 2 weeks the difficulty is recalculated to satisfy this requirement. If, for example, the number of mining nodes were doubled or the existing the number of mining nodes were doubled or the existing ones were to double their computational capacity, then the mining time would decrease, and in the established time period, the difficulty to obtain the hash would be recalculated on the rise.

To give an idea in terms of consumed energy, according to the data offered by **digiconomist**, **the annual consumption of electricity employed on Bitcoin[7] is that of 39.03 TWh**, which is of the same as the 39 TWh that was used to supply energy to all of Peru last year, according to **worlddata.info**.

## Proof-of-Stake (PoS)

PoS as well as the protocols we will mention next consist in assigning greater probability in winning the raffle to those that have more assets in the network -as amount of cryptocurrency-. Here, people are not competing to validate the block, and therefore, in general there is not a reward for who achieves it.

[7] **To the date of January 9, 2018.**

## Leased Proof-of-Stake (LPoS)

LPoS is a variation of PoS such that users with little capital can cede their probabilities of winning the raffle. In a case where the node that delegates ends up the winner and there is a reward for mining, it is divided proportionally between him and the people who supported him.

## Delegated Proof-of-Stake (DPoS)

DPoS is a variation of PoS where the nodes can propose any other node to validate blocks, which are known as witnesses, or to decide the characteristics of the same network such as time between or size of blocks, which are known as delegates. The more power a node has in a network, the more his vote counts. Each node proposes a number of enough nodes so that the network can be considered sufficiently decentralized, and the election is repeated after an established time period.

## Proof of Importance (PoI)

PoI functions like PoW but assigning the probability of being chosen in function to the activity, transactions, balance or reputation in the node's network instead of its money. The idea is the same, rewarding with the right of proposing blocks to the people that are most interested in the well functioning of the chain, so that it is not worthwhile for them to propose malignant blocks that could harm it.

So to say, in general the consensus protocols aim to have the person that proposes the block to be elected in a random manner, but in this election or raffle the probability that a node be selected is assigned in such a way that it is guaranteed that the selected person would not have an interest in misbehaving. For this, as we mentioned in the beginning, some blockchains demand to contribute computational capacity that leads to the chain's security and give a reward for it. Instead, other blockchains assign distinct probabilities to win the raffle of proposing the block in function of certain criteria such as the amount of money the chain's participants have, their activity in it, etc.

## Chain's security

There are three items to highlight regarding the chain's security.

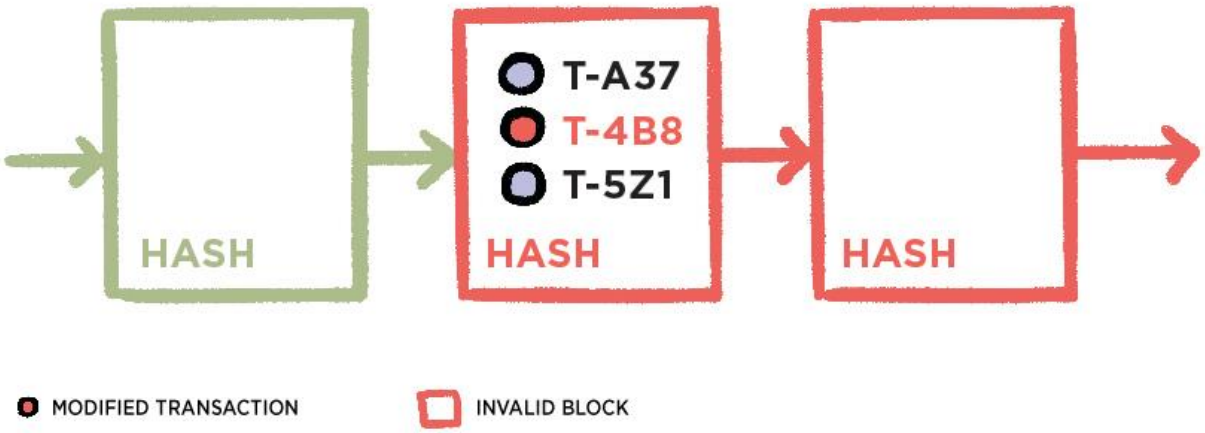
### a. Hash

The **hash is the code that is obtained by applying a mathematical function, known as the hash function, to a bunch of concatenated dat**a. A hash code is given to each group of data. The objective of using this hash in blockchain is to have all the information of each block in one alphanumeric code. This will permit us, as we will now see, to **detect changes in the blocks by just seeing the hash**.

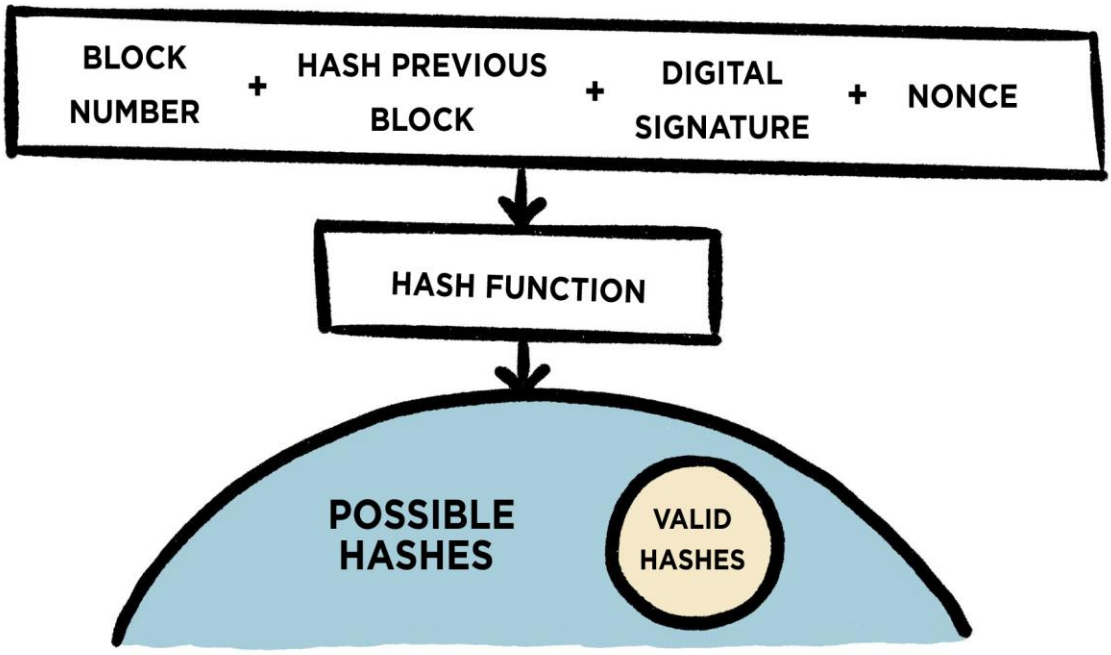
If, by now, we ask ourselves what information is needed to concatenate to obtain the hash, the quick answer is all the information of the block we wish to encrypt and to be able to detect changes in. In other words, the number of the block, the transactions it contains and the digital signature of the person who proposes to validate it, which are the constituting parts of the block such as it was defined before.

However, even though it is true that this permits having a unique hash for each block, in blockchain there are two more pieces that are essential in ensuring the chain's security.

The first piece is the hash code of the previous block. We have explained that **if something changes in any block, the hash is automatically going to change**, in such a way that if the previous hash was the one that we found as valid, the new one will be detected as tampered. If in the concatenation to obtain the hash code of each block, we introduce, along with the previous information, the previous block's hash, we then gather that if someone changes the information of one block, the hash of that block as well as the hashes of all following blocks became invalid. So to say, we propagate the error to all of the following blocks in the chain. **This allows us to detect any tampering or modification of any block in the chain by just looking at the previous block.**




The second piece to introduce is the nonce. **The nonce is a completely random alphanumeric code**. We said that the hash not only works to identify a block but that it also adds a layer of security. If we simply concatenate the block number, the transactions, the signature and the hash of the previous block to obtain the hash of each block, by applying the mathematical function we would always obtain the same hash because we are applying it to a fixed group of elements. Let's say, for example, that the hash code of a determined concatenation of data is 9ka41k3h5j18403k298g. What blockchain does is to demand that the hashes begin with a determined number of zeros so to be considered valid. For that purpose, a variable element has to be introduced, which is the nonce, which we concatenate with the rest. **The way to obtain a valid hash is therefore, to change the nonce in a random manner and apply the hash function until the result, the hash code resulting of the concatenation of all the elements mentioned before together with the nonce, begins with the demanded number of zeros**. If that was five zeros, a valid result would then be, for example, 00000x92ka7r91ja9k3.




What miners therefore do when the consensus protocol is PoW, is to try nonces in a random manner until obtaining a valid hash. The first to find it has the right to propose the following block, and if it is accepted, receives a reward in the form of a cryptocurrency previously agreed upon by the network. In Bitcoin, as we mentioned, the current reward is 12.5 Bitcoins and the average time to mine each block is 10 minutes.

## b. Capability to reject transactions and invalid blocks

**When each node receives a transaction, it automatically verifies that the involved operations are correct**. For example, that the person who makes a sale is the actual owner of what is being sold, and that everything is coherent and consistent. In the same way, so that a block is accepted it has to contain valid transactions and have a valid *hash*. In the case that a user is able to introduce a malignant block into the chain, lets suppose it was his random turn and he proposed a malignant version of a chain with an incorrect transaction, it would not be a catastrophe. If the next user randomly chosen proposes a block that is not ill-disposed as well, then he will propose his new version of the chain obviating the malignant previous block and adding in its place the one he proposes. The capacity to surpass the adversity of having a certain number of malignant individuals in a network that requires a consensus is known as the Byzantine Fault Tolerant.

## c. Consensus protocols, decentralization and game theory

**The consensus protocols allow to have a distributed ledger where different parts, without having to trust each other, can trust that the information they share and accept is valid**, and can also reject any information that isn't, in case it successfully enters the network. Moreover, given that PoW requires the employment of computational capacity to validate blocks and in PoS the *stake* will be penalized. This is an individual's "score" within a network. In case one acts in a negative way for the network, and taking into consideration that malignant behavior can be rejected by the rest of the participants, studies using game theory conclude that the most beneficial way for a person in a blockchain to act is always in benefit of the network, seeing that it will always be also in its own.

## Types of blockchain

Three different types of blockchain networks can easily be distinguished: public, federated and private. It is also worth mentioning *Blockchain as a Service* for cloud services.

Public. The public blockchain networks are those that **any person can access**. In general, the process to participate is to download the corresponding application and to connect, in an automatic manner, with a determined number of nodes who are asked for the most updated version of the chain. Once the node is up to date, it has the same rights and responsibilities as the rest of the participants when it comes to proposing and validating transactions, replicating the transactions it hears or mining, if they so wish. The safety of the majority of these is also based on consensus protocols and *hash* functions, and the users interact with the network in an anonymous manner.

Federated. The federated blockchains are a different network concept than the public ones and could even be considered a different technology, due to the fact that they do not satisfy, in many cases, the definition or description that we have tackled in the previous sections. **These blockchains have been arising with the idea of serving as decentralized ledgers that allow the generation of trust in complex environments with entities with different interests.** In general, they are not public. Instead, a **determined number of organizations, entities or corporations administer the network and keeping synchronized copies of the blockchain**. The generalized access is in this case through **a web interface** that the administrators make available to the users.

That is why it is of vital importance, at the time of designing and implementing this type of solutions, to **accompany the blockchain tool** with an adequate strategic plan consistent in defining **who are the participants, who and how the network will be administered, who will validate the transactions and what information will be made available to the web interface users.**

In many cases the user that accesses via web may not have an interest or any knowledge about blockchain but needs a platform that involves different entities and requires trust and transparency. A federated blockchain can then be a good option only if the established rules of the game in the administration and maintenance of the chain are the adequate ones and are offered to the user, through the web interface, to the degree of required transparency.

It is therefore clear, that by having access through the web and not as nodes with rights, the **common users will have as much access as it is decided to show them**. There will therefore bee alternatives that will vary from a large amount of transparency to a minimum amount of the same.

Block mining also acts here in a different manner. In general, the network does not even have an associated cryptocurrency, so that **the block-mining model with rewards that many public networks offer is no longer possible**. However, it is still necessary for the blocks to have a *hash*. Who then is in charge of finding it? One reasonable option is that the same organizations or entities in charge of the networks will be in charge of providing and maintaining servers that fulfill this purpose. So to say, **the mining work that is the heart of the public networks, that keeps them alive and is the users' responsibility, now takes second place and the network administrators are the ones in charge of providing the necessary computational resources to mine blocks** by finding hashes.

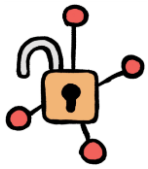
There are many options of open code to build a federated blockchain such as Hyperledger, Corda, EFW, or Multichain where you can download a blockchain application and program the chain to your liking, deciding who you would like to participate, under what rules the transactions are made, etc. The public networks like Ethereum or Litecoin also offer the opportunity to do a **fork**[8] to create federated or private environments.

Private. The private blockchains are those whose control is reduced to one entity that is in charge of maintaining the chain, giving permissions to users who wish to participate, proposing transactions and accepting blocks. They are the same as the federated ones but with only one entity in charge so that besides all of the differences in regards to the public ones that we already found in the federated ones, we must add that decentralization is lost.

*Blockchain as a Service* (BaaS): Some big companies offer cloud blockchain services. Some of these examples are IBM specialized in Hyperledger Fabric, Amazon collaborating with Digital Currency Group or Microsoft offering R3, Hyperledger Fabric or Quorum services, among others. These services not only consist in storing information, in this case of the blockchain, but their benefits also include an increase in security, not having to invest in hardware and the possibility of a more friendly working environment, being able to create your own blockchain channel without having to program.

**[8] A fork in which a new branch is temporarily created from a point of the blockchain, soft fork, or permanently, hard fork, that implements its own rules in regard to characteristics such as block size, for example.**

# Comparison between the types of blockchain




| | **Public**<br>Bitcoin, Ethereum, Litecoin | **Private**<br>Hyperledger, Corda, Quorum | **Federated**<br>Hyperledger, Corda, Quorum | **Blockchain as a Service**<br>IBM, Microsoft, Amazon |
|---|---|---|---|---|
| Anyone can join | ✓ | ✗ | ✗ | DA |
| In general, participants act as nodes | ✓ | ✗ | ✗ | DA |
| Transparency | ✓ | ~ | ~ | DA |
| Only one administrator | ✗ | ✓ | ✗ | DA |
| More tan one administrator | ✗ | ✗ | ✓ | DA |
| No administrators | ✓ | ✗ | ✗ | DA |
| No participant has more rights tan the rest | ✓ | ✗ | ✗ | DA |
| Smart Contracts can be implemented | ✓ | ✓ | ✓ | DA |
| Block mining rewards | ~ | ✗ | ✗ | DA |
| Solves trust problems | ✓ | ✗ | ~ | DA |
| Security based on consensus protocols | ✓ | ✗ | ~ | DA |
| Security based on hash functions | ✓ | ~ | ~ | DA |
| Provides cloud services | DA | DA | DA | ✓ |

✓ Yes ✗ No ~ Sometimes DA Does not apply

## Characteristics and applications of blockchain

Of the characteristics that convert blockchain into a useful tool **transparency, decentralization and no need for intermediaries** stand out.

- The concept of **transparency**, or the way it is obtained, varies in function to the type of network we are using. **In public networks, in general, there is total transparency** given that any user that registers to the chain is provided with a copy of the complete blockchain, and can see in it the current state of the assets and historical transactions. **In private and federated networks, access is restricted and via web for the majority of users, as we commented in the previous section. For these users the level of transparency is the one the administrators decide to offer them via website or app.**

- **Decentralization** is a determinant requirement when it comes to deciding if blockchain is or is not a good tool for a concrete case. To the extent that decentralization is desired, blockchain applies. If, instead, the problem demands a centralized database, then, in general, blockchain would not be the best option. Decentralization consists of basically determining the number of nodes that will maintain the chain. However, it is interesting to mention that this does not necessarily imply transparency, given that **the same nodes can have different roles within the system which give them a determined type of information, having the access vetoed to a certain content in the network.**

  Having distinct servers with a synchronized copy of the chain adds great value in terms of security, given that **if anyone modifies or corrupts one of the copies, it would be as simple as re-synchronizing it with the rest.**

- Regarding the **no need for intermediaries**, it is useful to highlight the words “no need”. Blockchain became known with Bitcoin to avoid the necessity of financial institutions intervening or verifying monetary, or cyptomonetary, transactions between individuals, so that the elimination of intermediation of the same was a desired and obtained objective.

  However, at the time of designing a private or federated blockchain the situation is different. It could be that in a system functioning with blockchain consistent in the delivery of a product from one place to another, **doing certain checks could be of interest to the stakeholders**. Let’s say, for example, that food products are being sent and they require certain humidity and temperature checks along their transport in car and boat. **Both parties would establish the accord, in a *Smart Contract*, of the parameters that must be evaluated during the checks and the payment that should be made in case everything continues its desired course.**

  These institutions could have their own node provided with only permission to see information regarding the temperature and humidity conditions that must be verified and could not know in any moment what is the accorded price for the shipment, for example. By satisfactorily finishing the established process in the *Smart Contract*, the money is automatically transferred to the seller.

It is therefore clear that blockchain is not a technological tool that offers a unique, non-flexible solution, but instead the complete opposite. Blockchain technology allows the construction of solutions that range from a centralized, non-transparent ledger to a decentralized network, with complex validation rules and a lot of transparency. That is why it is important to highlight the necessity of understanding blockchain not just as a solution to any problem but also as a tool that will be useful if employed in an adequate manner, which implies studying each case in an individual basis.

Among the numerous uses cases of this technology, it is interesting to see the possible applications in transparent and public political elections; registration of clothing or food manufacturing processes, which could be accessed via a QR code in the product; property ledgers, the governments of Georgia, Honduras or Sweden have been pioneers in this regards; all types of operations such as renting and selling of properties without need for intermediaries; border controls; medical registries; IPFS, inter planetary data stocking; and a long etc.

## Smart Contracts & IoT

Smart Contracts are a fundamental element of blockchain technology, given that they **establish and define how and who can make transactions**. They are contracts in which a series of clauses are defined and specified, such as the checks to be made by the shipment mentioned in the previous section and the final payment agreed upon in case the checks are positive. The difference with normal contracts is that these are **incorporated to a blockchain in a network, which guarantees its security and provides the adequate environment for their automatic processing.**

**IoT** is understood as the **network of things, instruments or devices connected to the Internet** that can range from a car to a washing machine. Different estimations calculate that in 2020, the number of devices connected to the Internet will be at least between 25 and 30 million. These devices are of great use as complementary to blockchain technology, given that they allow for the automatic confirmation of established clauses in the Smart Contracts, from measuring temperature to facial recognition. This accelerates, cheapens and optimizes the transaction process and the blockchain function. The smart devices that send information to the blockchain must have a digital identity that allows them to digitally sign said information, in case the information is not trustworthy. This is why not any device connected to the Internet is valid for blockchain.

## How to identify when blockchain is a useful tool?[9]

As we have been discussing, blockchain has some determined characteristics and offers concrete benefits. At the time of responding to whether or not blockchain is useful for a particular case, it is helpful to first consider that **blockchain is not a solution itself. Blockchain is a technological tool that has to be surrounded by a strategic plan that understands the needs of the project, identifies the degree of transparency and decentralization, determines the members that will act as nodes and establishes the adequate structure of the blockchain** defining how the transactions and/or the Smart Contracts will take place. Blockchain is a software that allows the creation of very different things, due to which its concrete implementation will be determined at the time of deciding whether it adds value or not.

**Essentially, blockchain will be useful as far as the case has a need for decentralization, an immutable ledger, transparency, consensus and validation.**

A way of seeing if blockchain is necessary and useful is to ask a series of questions such as the ones we will now describe and see if the previous five components are found within the answers. Given that there is currently a big interest in blockchain, it is often that people decide to do something with it without actually knowing what. Our recommendation is to start with a problem and see if blockchain can help within the solution. This takes us to the first question:

[9] **The strategic focus that is presented in this section corresponds to the work done by Mariana Gutierrez and will be further expanded on in future versions of this document.**

- What is the problem you are trying to solve?

  This avoids starting with “I want to use blockchain for something but I’m not sure what”. It is impossible to find a good solution if there is not a well-defined problem, and **it is impossible to know whether or not to use blockchain and how without knowing what for.**

- Who will have access to the blockchain? Who will administer the permissions?

  It is important to establish who and how the personas will participate in the network. **If a network is private or federated, the structure of nodes and the transactions that each one can process and/or validate will have to be cautiously designed.** Regarding the web access for the current users, in case they exist, it will also be important to study what they will be shown and how. It is not necessary for the user to know that behind the web interface there is a blockchain network same as he now doesn’t know if there is a database. Now, as we were discussing, if blockchain is wished to be used to increase transparency, the web interface will explicitly show it by, for example, depicting the hashes or the log of transactions.

- Do the personas belong to different categories (governments, corporations, workers, …)?

  **The more different the participants are, the more complex the consensus will have to be and more varied the transactions. There is where blockchain can help.** Each organization can play a different yet important role for the system.

  For example, for a network to register information about autos in a determined country, it could be that the government, the tax agency, the insurance companies and the big buy/sell auto companies are nodes in the network. On the other hand, each citizen would only have access through a web interface or an app to the data of their own car, and without having to be a node.

At the time of buying or selling, buyer and seller would inform the system via this website or app and the transaction would be validated by the insurance company, verifying that everything is in order regarding the insurance payments; the tax agency, taking note of the taxes and verifying that none of the parties have pending debts; and the corresponding ministry, which would approve and take note for its own ledger.

- Do the different participants trust one another? If not, what are the causes of dispute? Do they have different interests?

  Again, we must mention that **blockchain is of more use the more the interests are disperse, given that it will oblige the participants to come to an agreement in terms of the rules of the game**, as to how the permits, transactions and Smart Contracts will be made. **However, it is necessary to say that blockchain will not force the participants to stop being corrupt**, if these establish deficient rules of the game, which permit them to act in a malignant manner or if they concede validating permissions to entities that will not do their work in an honest way, blockchain will not be able to avoid it.

  From there we continue to emphasize **how important it is to enfold the blockchain tool with a good solution that will emerge from the correct study of a problem.** It is true that blockchain will always offer a ledger of the carried-out transactions and that, if it cannot avoid fraudulent behavior if a number of nodes agree to do so, at least the ledger remains and they will be forced to explain themselves.

- Are intermediaries involved? Who is in charge of validating? What are the rules for validation?

  The involvement of intermediaries is not a negative thing but it has to be well managed given that, as we have discussed, the entry door to system corruption is in the validations. **If an intermediary is given the possibility to validate, the most efficient and secure way for the network to do it will have to be studied.**

- What is the budget?

  Given that the technology is not thought out for small-scale solutions and that the possible implementations are so diverse and extensive, it is impossible to estimate a general budget regarding the possible cost of a solution using blockchain. It is, however, interesting to detail the different components of the solution.

  In regard to blockchain, resources to finance for initial stage of **the chain programming** and the **transaction mining** once it begins will be needed.

  Regarding the first, there are currently several free software options that any developer can use. The difficulty in the time of programming resides in the number of nodes that will participate, the number of assets that will be interchanged and the difficulty of the transactions or Smart Contracts that must be processed. For example, a solution using blockchain in which two companies exchange a unique certificate will be much less expensive than if a country government wishes to host the car ledger of the whole country, with multiple information exchange possibilities within them.

- Who will be responsible for mining?

  In terms of transaction mining it is important to differentiate if the blockchain will be on a public network or a private or federated one. **In the public networks, the mining and size of the block are predefined**, which is why **the validation cost of each transaction cannot be controlled** and will depend on each network. In the Ethereum network, the average rate per transaction at the end of 2017 was between one and two dollars, whilst in Bitcoin it reached 50. Even though many other public networks have much lower rates, an isolated environment could be more interesting for an ambitious project that requires a big volume of transactions. **In an isolated network, such as**

**the federated or private ones, the size of the block and the difficulty of the mining can be chosen.** Therefore, the cost could be given based on the number of computers needed, and in this case provided by the administrators, to mine the transactions from the network, without being conditioned by external agents.

In terms of transaction mining it is important to differentiate if the blockchain will be on a public network or a private or federated one. **In the public networks, the mining and size of the block are predefined**, which is why **the validation cost of each transaction cannot be controlled** and will depend on each network. In the Ethereum network, the average rate per transaction at the end of 2017 was between one and two dollars, whilst in Bitcoin it reached 50. Even though many other public networks have much lower rates, an isolated environment could be more interesting for an ambitious project that requires a big volume of transactions. **In an isolated network, such as the federated or private ones, the size of the block and the difficulty of the mining can be chosen.** Therefore, the cost could be given based on the number of computers needed, and in this case provided by the administrators, to mine the transactions from the network, without being conditioned by external agents.

The type of network, the number of nodes and the amount of transactions are the three aspects to keep in mind in terms of the blockchain tool but they do not constitute the whole solution. In the complete solution it would be necessary to connect blockchain with a **web interface** that would have also been designed and implemented, and in the majority of the cases accompanied with a **database** that hosts the documents, given that in the blockchain only the hashes are stocked.

Currently, most of the projects employing blockchain are in pilot mode, which seems the most advisable to start given the premature phase of the technology and the very probable large scope of the solution. Several companies offer to run a pilot within the period of 3 months.

## How to begin to construct a solution with blockchain?

Once the problem that wants to be resolved is clearly defined; the degree of decentralization, transparency, consensus and validation have been analyzed; the participants have been identified; and the conclusion that blockchain is the adequate tool to begin to solve the problem has been reached, it is time to start using said tool.

A way to do so is to classify the elements that will be involved in the solution into three groups. First, we will define them and then we will see an example:

- **Participants:** The participants are all those collectives that will play a role, from the corporations that administer the network, in case there are any, to the users going through auditing entities, financial institutions, etc. The question to be made is **who is each persona, which are the permissions they have over the network**, so to say, if it will interact with it through a website, if it will keep a copy of the chain, if it will only be able to see the transaction in which it participates or if it will have access to more information, etc., and **which transactions it will be able to make.**

- **Assets:** Once it is clear who will participate, we need to know **what they will be exchanging**. Maybe it seems a bit abstract now, but the way to understand this group is to think that **when the participants make a transaction they are certainly trading something**. This something is the asset, and it can range from being a certificate or document. In reality, in blockchain the documents themselves are not kept, but their *hash*, a token that gives for example the right to vote in an election, a certification, etc. is.

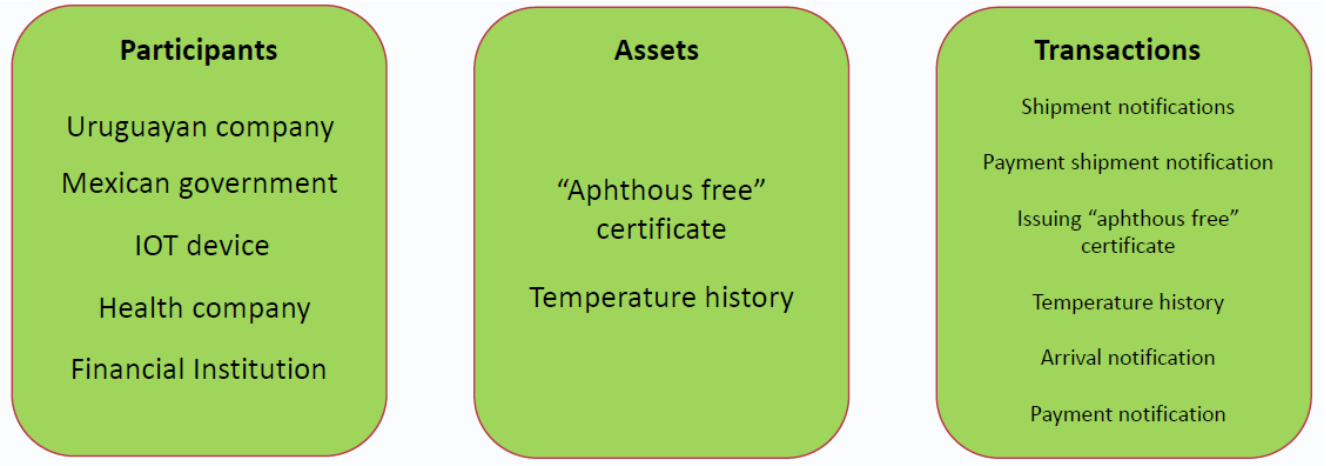
- **Transactions:** The third element is the transactions. If we already know who is going to "play" and what are the "toys", we still have to define what the rules of the game will be. Without the transactions, we have everyone excited with no way to move, and these are the ones that allow the wheels to start turning. The transactions are **the operations via which the participants create, exchange, modify or destroy assets.** Besides, by defining the transactions we can also **specify what participants have permission to do during a specific transaction and which are the necessary validations** so that this transaction can be processed and added to the blockchain. As we have been maintaining in this document, a transaction is actually any change or update that happens in the network that is picked up by the blocks of the blockchain.

Let's look at an example. Let's suppose that a Uruguayan company wants to export a meat cargo to Mexico. The Mexican government demands that the meat be certified as aphthous free and that it does not surpass a determined temperature during the journey. With this objective, a periodic temperature check will be done each, let's say, 15 minutes in the container that carries the meat. If the meat arrives to Mexico with the aphthous free certification and without having surpassed the demanded temperature, the Mexican government shall then make the agreed upon payment to the Uruguayan company. How would this case be a solution using blockchain? Who are the participants, the assets and the transactions?

- **Participants:** The exporting Uruguayan company, the Mexican government, a financial entity that will keep Mexico's money while the shipment is en route, an IoT device that will send periodic information about the container temperature, a certifying entity that proves the shipment is aphthous free and emits the corresponding certificate and a possible auditing entity that supervises the whole process.

- **Assets:** Here, the assets could be the aphthous free certificate and the temperature history of the container measured by the IoT device that is issued just in case that the temperature never surpassed the desired degree.

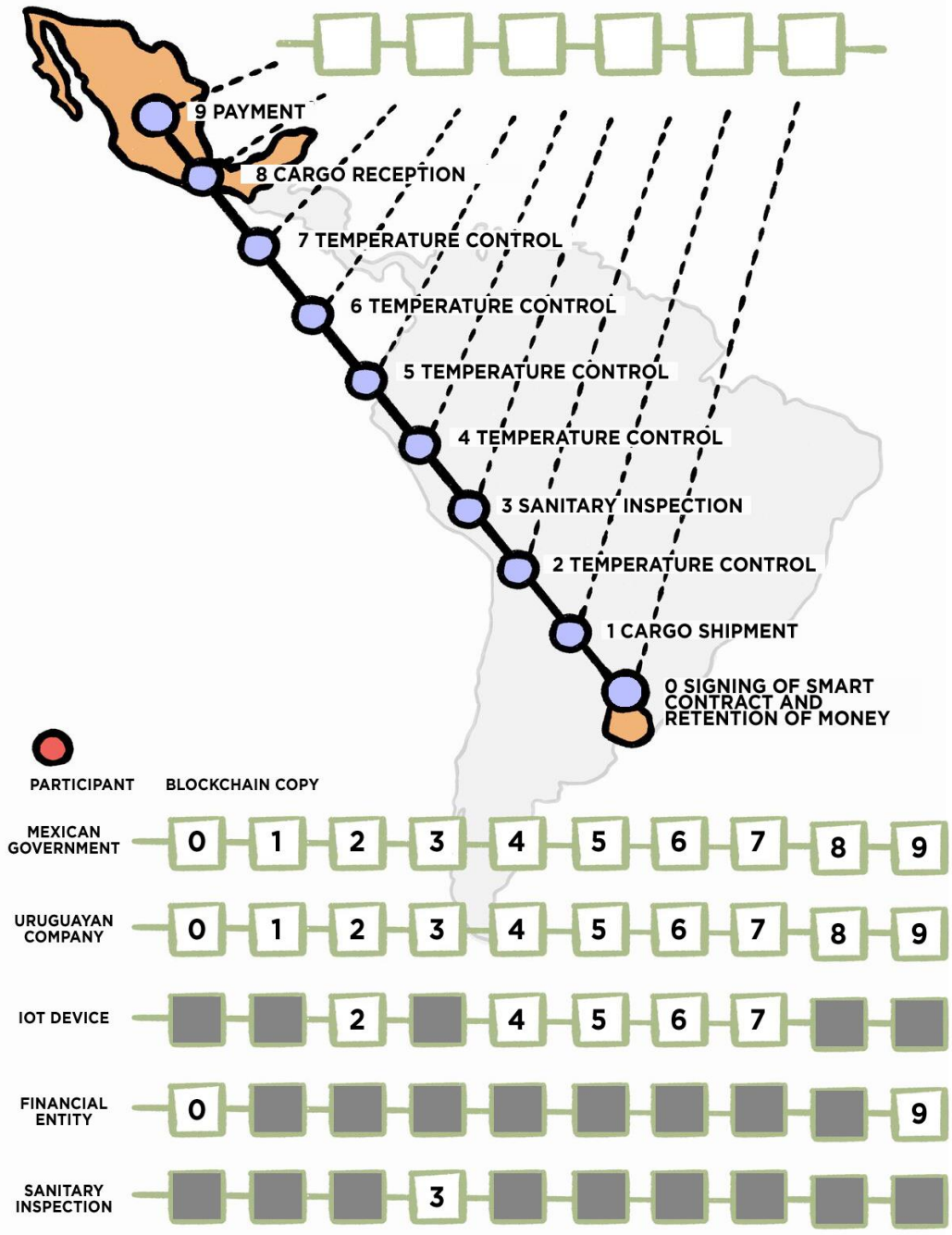
- **Transactions:** The transactions could be the shipment notification from Uruguay, the payment deposit notification, the issue of the aphthous free certificate, the periodic temperature measurements from the IoT device, the arrival notification and the payment notification.




The way the process will then take place is the following:

0. The Uruguayan company and the Mexican government sign an agreement, in the form of a Smart Contract, through which the previous clauses are implemented in a blockchain, and the Mexican government saves the agreed upon sum in a corresponding financial entity to be sent if everything goes according to plan.
1. The exporting Uruguayan company sends the cargo and notifies the blockchain.

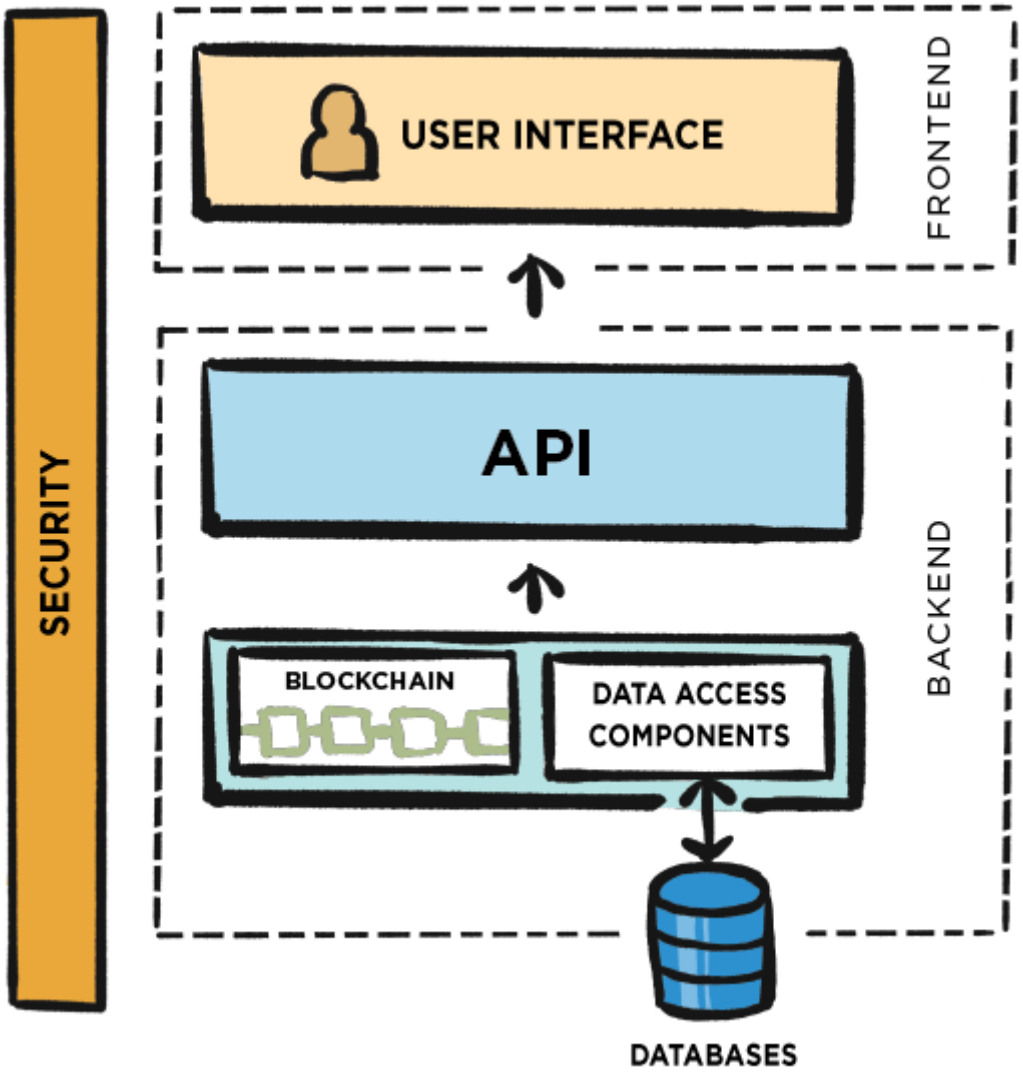
2. The assigned entity verifies that the product is in the required conditions and issues the aphthous free certificate that is then registered in the blockchain.
3. The IOT device put in the interior of the container measures the temperature and sends it every 15 minutes.
4. The container arrives to the Mexican government, issuing the corresponding notification in the blockchain.
5. The financial entity that had retained the Mexican government's money frees it to give to the Uruguayan company.


9 PAYMENT
8 CARGO RECEPTION
7 TEMPERATURE CONTROL
6 TEMPERATURE CONTROL
5 TEMPERATURE CONTROL
4 TEMPERATURE CONTROL
3 SANITARY INSPECTION
2 TEMPERATURE CONTROL
1 CARGO SHIPMENT
0 SIGNING OF SMART CONTRACT AND RETENTION OF MONEY
PARTICIPANT
BLOCKCHAIN COPY
MEXICAN GOVERNMENT
0 1 2 3 4 5 6 7 8 9
URUGUAYAN COMPANY
0 1 2 3 4 5 6 7 8 9
IOT DEVICE
2 4 5 6 7
FINANCIAL ENTITY
0 9
SANITARY INSPECTION
3

## Blockchain architecture

Throughout the document we have insisted that blockchain is not a solution, but a tool. **The solution is composed by the entire process consistent in at least understanding the problem, identifying the actors, selecting the technology and the implementation of such.**

It is convenient to indicate that in a solution that uses blockchain, it will often find itself with another two components besides blockchain, these are web interface and database.



We have talked in detail about how in federated and private networks the custom is to have a **web interface** through which the users interact with the system. Along those same lines, it is also necessary to indicate that heavy documents do not get stored in the blockchain but in a **database**, where the hash resulting of encrypting the document and what is therefore stored in the blockchain.

A simple diagram that illustrates a generic architecture could be the one presented in the previous page. In the proposed design, users are given web or mobile access that consumes an API. Underneath, we have the blockchain and a layer of data access that takes care of, just in case, of controlling the information exchange with the database. The generic user would have its username and password to access the information in the web interface and only the designated entities would have a copy of the blockchain and access to the databases.

## Anonymity

In the federated and private networks that have a social, business and/or commercial purpose, the personas are either well-identified organizations or accredited users with access via the web. In general, anonymity is non-existent.

In the public networks associated with cryptocurrencies, however, the users interact with the blockchain in an anonymous manner. They register with a private key and show the other users their public key. Nevertheless, given that all of the history is public, it would suffice to associate the real identity of a person with its public key one time to be able to follow their tracks.

To avoid discovering the real identity of a user in the anonymous networks, some blockchains implement certain internal processes to “mislead”. Some crypto-based networks implement a process called mixing, through which different transactions of the same amount between nodes are entered into a “black box” that crosses the senders’ and recipients’ wallets in a random manner, therefore avoiding being able to identify where each comes from and consequently erase their tracks. Some cyrptocurrency networks have the capacity to implement this type of processes in the same code of the network and the possibility of doing it in each transaction is made easier.

It is also interesting to comment that even if it may seem that each node being connected to the rest, unlike the actual peer-to-peer schema, seems like the most efficient thing, this would go against anonymity. If each node were to be connected with all of the rest, when one node receives information of a transaction it would know that the person doing it is precisely the person sending it to him. This would allow it to relate the sending node’s IP with the public key in the transaction and therefore could easily identify the real identity of the anonymous users.

## Conclusions

During the last years, blockchain has become one of the most interest-generating technologies in the world. Governmental institutions, international organizations and big corporations are trying to build solutions using blockchain.

Although the technology, even though ingenious, is not excessively complex, building a big-scale solution where each participant understands, respects and performs their function is. This is why, as a project gains scope the challenges are not only technological but they also reside in joining all of the actors under a same consensus and rules.

This document has tried to explain the functioning of blockchain, highlighting the characteristics that make it a different technology. We have also wanted, however, to make clear that blockchain is not a solution but a tool and that consequently just like a hammer is good at hanging nails but not at putting in screws, blockchain is not always the best option. A way of starting to discern if blockchain would be useful in a determined case is to ask ourselves a series of questions such as we established in the section: *How to identify when blockchain is useful*.

Once the problem is well established and the solution is identified, one can organize and structure it. In the case that a solution has a blockchain component, a possible form of doing it has been given in the section: *How to start to build a solution with blockchain.*

It is also worth mentioning that in big-scale projects validation and learning are important in intermediate phases. This is why, once the previous two steps have been done and before going onto production, we have recommended to start with a pilot that puts the designed prototype into practice, validates that the participants know how to interact with the solution, that they do so in the correct manner and that it contributes to what they desire.

Regarding the challenges that blockchain will have to confront in the future, it is necessary to talk about the introduction of new quantum technologies. These, as we will discuss in detail in the next publication, will completely change the encryption and cyber security techniques in the next decade. If blockchain technology could continue to be secure and useful it will have to succumb to certain changes in order to adapt to this new era.

Without a doubt, in the next years we will see if blockchain is here to stay or if it is a trend. In any case, it is a smart idea that deserves to be explained, understood and explored.

# ANNEX: CRYPTOCURRENCIES

## Cryptocurrencies

Bitcoin is born in 2009. Given its success, many other crypto-based blockhain have been created since. Currently there are more than 2000 cryptocurrencies in circulation. Until up to a few months ago, September 2017, Bitcoin monopolized 50% of the total capitalization of cryptocurrencies and the majority of the daily market volume. In the last two months, December 2017 and January 2018, there has been an authentic fever first with Bitcoin and then with a big quantity of alternate cryptocurrencies, known as Altcoins.

Bitcoin started with a price of 0.06 per unit[10]. Currently, its value is $15,261.80. As you can see in the image, the first years its price increased in a moderate manner until the end of 2013, where it had its first exponential growth. At the end of 2017, the second exponential growth took place, shooting its price from $2,735.99 on August 1, 2017 to more than the $19,535.70 it reached on December 17 of the same year. This represents a 714% increase, which means its value increased 7.14 times in just four and a half months.


[10] All the data relative to cryptocurrencies, as well as the graph, are courtesy of https://coinmarketcap.com.

To put into perspective, in the same time period Amazon stock options increased from $996.19 to $1,174.14, which is equivalent to a 118% increase, so to say, practically 7 times less profitable[11].


***Amazon stock price evolution from January 2017 to January 2018.***

La capitalización de mercado a día 9 de enero de 2018 es de casi $257.000 millones, con un volumen diario de unos $20 millones. En el último mes el número de criptomonedas con más de $1.000 millones de capitalización de mercado era 12, mientras que ahora ya son 43.

The market capitalization up to the date of January 9, 2018 is that of $257,000 million, with a daily volume of about $20 million. In the last month the number of cryptocurrencies with more than $1,000 million of market capitalization was 12, while now it is 43.

[11] **The source of the data and graph corresponding to Amazon stock are from https://www.nasdaq.com.**

## What is the use of cryptocurrencies?

Like any fiduciary currency, cryptocurrencies serve as an asset in which to invest and as a payment method.

**Investment:** Given its general increasing tendency, the most seated cryptocurrencies have been a good investment at medium term. Short term, their 24-hour volatility has come to be around 10% on average. Given that the longer ones have only had a life span of nine years, there are no precedents as to what can happen in the long term.

**Payment method:** Currently some of the most well-known companies that accept Bitcoin are Expedia, eGifter, Save the Children, Microsoft, Overtsock.com, Newegg, Shopify stores, Wikipedia, Peach Airlines or Tesla. Other companies such as Amazon are evaluating the possibility of also incorporating it. Maybe in the future some local commerce or small industries will also join the initiative.

## Ways of obtaining cryptocurrency coins

In general, there are four ways of getting cryptocurrency.

**1. Genesis Block:** When a cryptocurrency is created, generally a coin is sent to a determined number of participants in the first block with the intention of motivating them to use it. This is the only way to obtain a “free” cryptocurrency.

**2. Minning:** In the networks that serve as a PoW, and in some that use PoS, the users that employ computational capacity to obtain the hash of the blocks are rewarded with a coin. As was mentioned in the protocol consensus section, only the winner of the competition is rewarded. In the more important cryptocurrency blockchains the people are organized in mining pools, which are groups of people joining computational resources under the supervision of a manager that divides the rewards in proportional parts in case of a successful mining. This makes it more difficult for isolated miners to be successful and opens up the debate about real decentralization in the network.

**3. Transaction Fees:** The different nodes that make transactions or other operations that need to be mined by the community can leave a reward for the person in charge of mining. In Ethereum they are known as gas and depend on the difficulty of each transaction or Smart Contract. In Bitcoin, if they were not something relevant until a while ago, with the current congestion of transactions, these "interests" for the miners have skyrocketed. It is necessary to mention that all cryptocurrency emissions are finite so that the quantity of issued currency be fixed and therefore when the mining reward comes to its end, it is expected that these commissions keep motivating the miners to validate transactions and blocks.

**4. *Trading*:** Like any asset, one can always be interchanged for another, be it fiduciary money, a cryptocurrency or anyone that is willing to do it. There is a multitude of trading houses in the network that facilitate a friendly interface through which obtaining a virtual wallet with which to buy and sell cryptocurrency. The counterpart is that they demand proof of identity, they charge commission and if they are hacked and they steal the address of your wallet from their page you lose all of your money. To buy Bitcoin, Ethereum, Bitcoin Cash or Litecoin the most used are Coinbase and Kraken. In them you can acquire these cryptocurrencies in exchange for real badges. To invest in less common Altcoins we have to use Bitcoin or Ethereum, which are generally acquired from the recently mentioned web pages, and send them as Binance or Kucoin where they can be traded for other currencies.