Índice

[1. Introducción 2](#_Toc5358718)

[1.1. Presentación del problema 2](#_Toc5358719)

[1.2. Subtitulo 2 3](#_Toc5358720)

[1.1.1. Subtítulo 2 3](#_Toc5358721)

[2. Un poco de contexto. Blockchain 4](#_Toc5358722)

[2.1. Características 4](#_Toc5358724)

[2.2. ¿Qué es un bloque? 4](#_Toc5358725)

[2.3. ¿Dónde están los bloques? 5](#_Toc5358726)

# Introducción

¿Por qué Blockchain? ¿Si ya tiene más de 15 años, qué trae nuevo? ¿Por qué he de fiarme de algo que se califica a sí mismo como inmutable? ¿Pero es seguro? En la era de las APIs, ¿por qué debo de fiarme de un Smartcontract? Pero y eso de un Smartcontract, ¿qué es? ¿Necesito cambiar las competencias del equipo de desarrollo? Y además, ¿debo invertir en criptomonedas para poder hacer mi aplicación empresarial? Etc…

Estas cuestiones y otras muchas, son las que cualquier analista, jefe de proyecto, responsable de TI o incluso de negocio que se enfrenta a un nuevo desarrollo, podría llegar a hacerse cuando ha de abordar al reto de diseñar e implementar un proyecto, que de solución a una necesidad de negocio o administrativa, en un entorno corporativo. Pues bien, de entre los varios objetivos que se han planteado a la hora de realizar el presente trabajo, está el de dar respuesta a todas estas preguntas. … *a través de la presentación de dos desarrollos realizados con esta tecnología, que poco a poco está introduciéndose en muchos de los sectores económicos e industrales del mundo entero, y que en muchas ocasiones viene a simplicar procesos.*

## Presentación del problema

En la actualidad, o mejor dicho desde hace ya bastante tiempo, estamos viviendo en la era de la interconexión, y no solo a nivel personal, sino también a nivel empresarial y administrativo. Por ejemplo, los bancos quieren que sus clientes tengan un seguro de vida cuando contratan una hipoteca, y la mayoría lo hacen a través de compañías aseguradoras que les proporcionan la información sobre las coberturas y el precio de la póliza; compramos un billete de avión y reservamos una habitación de hotel en una plataforma online, esta web previamente ha necesitado consultar la disponibilidad de plazas y precios a la compañía aérea y al hotel de alojamiento; no dirigimos a la administración y junto a nuestros datos fiscales aparecen los laborales o los de la Seguridad Social. Se podrían poner multitud de ejemplos, pero en todos existe un denominador en común, la interconexión. En la actualidad los sistemas necesitan compartir información y funcionar en un ecosistema abierto, ya sea dentro de la propia organización o hacia afuera.

¿Pero son todos los sistemas compatibles? ¿Funcionan todos con los mismos mecanismos de seguridad? ¿El formato de la información es el mismo?

|  |
| --- |
| Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. |

Subtítulo 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## Subtitulo 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

### Subtítulo 2

* Viñeta 1
  + Subviñeta 1.1
* Viñeta 2
  + Subviñeta 2.2
* Viñeta 3
* Viñeta 4

# Un poco de contexto. Blockchain

¿Pero qué es Blockchain? La respuesta es, una red P2P (*peer-to-peer*) en la que se crean transacciones digitales, y que funciona como un libro mayor de contabilidad o *ledger*. En esta red la información se almacena en bloques, en donde cada uno de ellos contiene información relativa al bloque anterior, lo que permite ir formado una cadena.



## Características

Esta “cadena de bloques” posee las siguientes características:

* **Descentralizada** (*Trustless*): Todos los nodos son responsables de la gestión y modificación de la información al mismo tiempo. Esto significa que cualquier servicio o aplicación seguirá funcionando si un nodo o grupo de nodos deja de estar disponible, en este caso la información seguirá fluyendo al persistir en el resto de nodos de la red.
* **Distribuida** (*Many to many*)**:** Cualquier nodo perteneciente a la blockchain está conectado al resto de nodos de la red. Con la aplicación estricta de este concepto, en una Blockchain se hace casi imposible manipular los datos almacenados en ella, dado que todos los nodos tiene una copia de los mismos y los cambios no permitidos podrían ser rechazados al ser dados como *no válidos*.
* **Consistencia de datos** (*Proof of work*)**:** Tanto en **Bitcoin** como en **Ethereum** los nodos pertenecientes a la red verifican la validez de cada transacción realizada en ella, a través de un **algoritmo de consenso**. En el caso de estas dos redes, este algoritmo se denomina ***Proof of Work***. En capítulos posteriores, y después de haber introducido algunos conceptos de criptografía, profundizaremos en este concepto.
* **Inmutable** (*Ledger*)**:** Los datos almacenados en la red no pueden ser eliminados. Podrán ser modificados en posteriores operaciones, pero siempre existirá un registro histórico con todos los datos a través de la cadena de bloques.

## ¿Qué es un bloque?

Según se define en <https://www.sinergiablockchain.org/_/Doc/FAQ.pdf>:

*“Un bloque es un conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques. Cada bloque que forma parte de la cadena (excepto el bloque generatriz, que inicia la cadena) está formado por:*

* *Un código alfanumérico que enlaza con el bloque anterior.*
* *El “paquete” de transacciones que incluye (cuyo número viene determinado por diferentes factores).*
* *Otro código alfanumérico que enlazará con el siguiente bloque.”*

La imagen siguiente (*Figura 1*) muestra el concepto de una “cadena de bloques”.

**Block Hash: 0000078ecba1500**

**Previous Block Hash: 0000096effa4600**

**Block Hash: 0000011aee0534e**

**Previous Block Hash: 0000078ecba1500**

**Block Hash: 000056abff1189a**

**Previous Block Hash: 0000011aee0534e**

**Transaction Hash: 000aa76effa4133**

**Transaction Hash: aaf4000faee3a00**

**Bloque 76**

**Bloque 77**

**Bloque 78**

Figura 1: Representación de la cadena de bloques.

Pero como en todo siempre hay un principio, y una cadena de bloques no es una excepción, existe un bloque generatriz denominado Génesis, a partir del cual se encadenan el resto.

## ¿Dónde están los bloques?

Los bloques se sitúan en los NODOS. Estos no son más que los ordenadores que componen la red, en donde reside un software