



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



# **BLOCKCHAIN: APLICACIONES A LA ADMINISTRACIÓN PÚBLICA**

TRABAJO FIN DE GRADO

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

**AUTOR:** FRANCISCO CAMPOS MÍNGUEZ

**TUTOR:** JOSEP DOMÉNECH I DE SORIA

CURSO ACADÉMICO: 2018-2019



## Tabla de contenidos

<b>1. INTRODUCCIÓN:</b> .....	<b>6</b>
1.1 RESUMEN .....	6
1.2 ABSTRACT .....	7
1.3 MOTIVACIÓN .....	8
1.4 OBJETIVOS .....	8
1.4.1 OBJETIVO PRINCIPAL.....	8
1.4.2 OBJETIVOS SECUNDARIOS .....	8
1.5 ESTRUCTURA DEL TFG .....	9
<b>2. MARCO CONCEPTUAL</b> .....	<b>10</b>
2.1 DEFINICIÓN DE BLOCKCHAIN.....	10
2.1.1 INTRODUCCIÓN A BLOCKCHAIN.....	10
2.1.2 FUNCIONAMIENTO DE BLOCKCHAIN .....	15
2.1.3 PROTOCOLOS DE CONSENSO.....	16
2.2 ETHEREUM .....	18
2.2.1 SMART CONTRACTS .....	21
2.2.2 ETHEREUM VIRTUAL MACHINE.....	22
2.2.3 GAS EN ETHEREUM.....	23
2.3 BLOCKCHAIN Y EL SECTOR PRIVADO.....	25
2.3.1 INTERNET DE LAS COSAS.....	28
2.4 TECNOLOGÍA BLOCKCHAIN Y LA INDUSTRIA ENERGÉTICA.....	30
2.4.1 POSIBLES APLICACIONES DE BLOCKCHAIN EN EL SECTOR ENERGÉTICO .....	31
2.4.2 CONCLUSIONES.....	33
<b>3. BLOCKCHAIN EN LA GESTIÓN PÚBLICA</b> .....	<b>34</b>
3.1 PROYECTOS BLOCKCHAIN EN LAS AAPP .....	34
3.2 BLOCKCHAIN Y LA JUSTICIA DESCENTRALIZADA .....	34
3.2.1 JUSTICIA EN LAS PRIMERAS SOCIEDADES .....	34
3.2.2 KLEROS, JUSTICIA DESCENTRALIZADA. ....	35
3.2.3 CONCLUSIONES.....	37
3.3 BENBEN A TRAVÉS DE BLOCKCHAIN .....	37
3.3.1 DESARROLLO DE BenBen .....	37
3.3.2 CONCLUSIONES.....	39
3.4 BLOCKCHAIN Y LA AUTORIDAD MONETARIA DE SINGAPUR .....	40
3.5 BLOCKCHAIN EN EL SISTEMA SANITARIO.....	43
<b>4. BLOCKCHAIN EN LA GESTIÓN DEL SISTEMA DEMOCRÁTICO</b> .....	<b>47</b>
4.1 BLOCKCHAIN Y EL VOTO ELECTRÓNICO .....	47
4.1.1 SISTEMA ELECTORAL ESPAÑOL EN LA ACTUALIDAD .....	47
4.1.2 ELECCIONES CON BLOCKCHAIN.....	50
4.1.3 ESTONIA EL PAÍS DIGITAL POR ESCELENCIA.....	51
4.1.4 ¿POR QUÉ EL VOTO ELECTRÓNICO NO ES UNA REALIDAD EN NUESTRO PAÍS?.....	54
4.1.5 CONCLUSIONES.....	55
4.2 CATALUÑA Y BLOCKCHAIN .....	56
4.2.1 PROYECTO “loCat” .....	58
4.3 TIVI .....	58

5. CONCLUSIONES .....	61
BIBLIOGRAFÍA .....	66

## Índice de figuras

FIGURA 1- REPRESENTACIÓN VISUAL DE LAS REDES COMENTADAS .....	13
FIGURA 2. DIFERENCIAS ENTRE BLOCKCHAIN PÚBLICAS Y PRIVADAS.....	14
FIGURA 3. COTIZACIÓN DE ETHER .....	19
FIGURA 4. ORDENADORES CONECTADOS POR INTERNET FORMANDO LA ETHEREUM VIRTUAL MACHINE .....	23
FIGURA 5. GRADO DE DESARROLLO DE APLICACIONES BLOCKCHAIN EN EMPRESAS PRIVADAS .....	25
FIGURA 6. SECTORES QUE LIDERAN EL DESARROLLO DE BLOCKCHAIN .....	26
FIGURA 7.- MULTINACIONALES CON MAYOR NÚMERO DE PATENTES DE BLOCKCHAIN EN SU PODER .....	28
FIGURA 8- KLEROS COMO RED DE ADJUDICACIÓN DESCENTRALIZADA .....	36
FIGURA 9.- SANIDAD PÚBLICA Y PRIVADA CON BLOCKCHAIN .....	45
FIGURA 10- REPARTO DE ESCAÑOS DE DIPUTADOS POR PROVINCIAS .....	48
FIGURA 11- REPARTO DE ESCAÑOS A TRAVÉS DE LA LEY D`HONDT .....	49
FIGURA 12- LA CARRETERA X-ROAD .....	52
FIGURA 13.- VOTO ELECTRÓNICO CON BLOCKCHAIN .....	54

## Índice de tablas

TABLA 1.- VOLATILIDAD DE LAS 4 CRIPTOMONEDAS MÁS CONOCIDAS DEL MOMENTO .....	20
TABLA 2.- CONTRATO TRADICIONAL VS SMART CONTRACT .....	22
TABLA 3.- POSIBLES USOS DE BLOCKCHAIN EN EL SECTOR ENERGÉTICO.....	32
TABLA 4.- REDUCCIÓN EN LOS TIEMPOS DE ESPERA GRACIAS A BENBEN .....	39

## 1. INTRODUCCIÓN:

### 1.1 RESUMEN

Actualmente la palabra blockchain o cadena de bloques ha cobrado verdadera importancia en muchos ámbitos de la sociedad en la que vivimos. Esta ha llegado a nuestros oídos principalmente porque Bitcoin la utiliza y por su crecimiento de manera exponencial en el ámbito financiero. Pero esta tecnología no se limita a estos aspectos y tiene mucho más que aportarnos. Gracias a sus características inherentes puede ser muy útil para las instituciones y las Administraciones Públicas.

En una sociedad en la que el fraude y el soborno han hecho que la reputación de estas administraciones se vea debilitada, tecnologías como blockchain pueden ayudar a mejorarla, garantizando transparencia e integridad en los procesos públicos y con ello aumentando la seguridad y confianza ciudadana hacia estas instituciones.

A lo largo de este trabajo desarrollaremos la cadena de bloques para posteriormente centrarnos en los posibles usos de esta en los ámbitos más importantes de la Administración Pública. Analizaremos como blockchain puede mejorar los servicios prestados por estas administraciones con el fin de mejorar el servicio prestado a los contribuyentes. Y comprobaremos como esta tecnología será parte importante de nuestras vidas tanto laborales como personales al introducirse en multitud de empresas e instituciones públicas para la mejora de los servicios prestados por estas.

**Palabras clave:** cadena de bloques, administración pública, criptomoneda, identidad digital, inmutabilidad, economía digital, seguridad.

## 1.2 ABSTRACT

Currently, the word “blockchain” has gained a considerable importance in several spheres in the society we live in. This word has been known because Bitcoin uses it and it has grown exponentially in the financial field. However, this technology is not only limited to this aspects, therefore it has a wide range of possibilities. Thanks to these inherent characteristics, it can be very useful for the institutions and Public Administrations.

In a society in which fraud and subornation have caused the enfeeblement of these administrations, technologies like blockchain can help to improve it by ensuring transparency and integrity in the public processes. As a consequence, civic security and confidence grow towards these institutions.

Throughout this project, block chain will be developed in order to focus on the possible uses of this technology in the most important fields of the Public Administration. Block chain will be analysed to see how to improve the services offered in these administrations with the goal of improving the services offered to the contributor. Finally, this technology will be checked as an important part of our labour and personal life, since it will be introduced in a multitude of companies and institutions in order to improve the services offered by them.

**Key words:** blockchain, public administration, digital currency, digital identity, inmutability, digital economy, safety.

## 1.3 MOTIVACIÓN

Tras los conocimientos adquiridos en el Grado de Administración y Dirección de Empresas de la Universidad Politécnica de Valencia junto con lo aprendido en cursos oficiales impartidos por esta misma institución, en dicho TFG se quiere demostrar las habilidades desarrolladas durante estos cuatro años en los que he crecido y formado como profesional y como persona.

A lo largo del grado he tenido la oportunidad de participar en diversas charlas y cursos sobre diferentes temas, y uno de los ámbitos que más despiertan mi curiosidad son las finanzas y dentro de las finanzas las inversiones en bolsa. Siempre recordaré uno de esos cursos sobre inversiones en bolsa donde uno de los speaker nos introdujo la palabra blockchain animándonos a estudiar más sobre este tema si alguna vez teníamos la oportunidad porque desde su punto de vista sería de gran relevancia en muchos de los sectores de nuestra futura vida profesional.

Cuando tuve la oportunidad de elegir el tema sobre mi TFG no dudé ni un instante que estudiar la cadena de bloques sería muy interesante y me ayudaría a comprender mejor un término y una tecnología que cada vez son más frecuentes en nuestro día a día y que puede que sea una parte importante de mi futura vida laboral, así que en ello he basado este trabajo en esa curiosidad sobre este ámbito y en las ganas de aprender algo nuevo que quizás dentro de unos años se convierta en básico en nuestro día a día.

## 1.4 OBJETIVOS

En este pequeño apartado vamos a introducir los objetivos que hemos considerado relevantes a la hora de realizar este trabajo.

### 1.4.1 OBJETIVO PRINCIPAL

El objetivo principal del presente trabajo final de grado es conocer y entender la tecnología blockchain para comprender el potencial y usos que puede generar en las Administraciones Públicas del Estado, ayudando a estas a ofrecer unos servicios con mayor transparencia y participación ciudadana y mejorando la eficiencia de los mismos para ahorrar en costes para el Estado y en mejora de los servicios para los ciudadanos.

### 1.4.2 OBJETIVOS SECUNDARIOS

- Para poder desarrollar las aplicaciones a la administración pública es necesario conocer primero como funciona la tecnología.
- Estudiar los tipos más importantes de cadenas de bloques para ser capaces de comprender que funcionalidades puede aportar a las Administraciones Públicas del Estado.
- Analizar usos ya existentes en otros ámbitos que no sean de la administración pública, pero que puedan enfocarse en un futuro hacia ella.
- Comprender todo el potencial de esta tecnología en los servicios públicos.

## 1.5 ESTRUCTURA DEL TFG

El presente trabajo final de grado ha sido estructurado atendiendo principalmente a las diferentes partes de la sociedad donde blockchain puede aportar sus funcionalidades.

En primer lugar el primer capítulo, donde se encuentra este epígrafe “Estructura del TFG, hemos desarrollado entre otras cosas el resumen, el objetivo y objetivos secundarios del TFG además de hablar de la motivación que nos ha llevado a desarrollar este proyecto.

En segundo lugar en el epígrafe dos “Marco Conceptual”, hablamos de la tecnología de la cadena de bloques con todas sus características básicas, también desarrollamos la plataforma Ethereum y su funcionamiento y hemos finalizado el capítulo desarrollando como puede y está actuando blockchain en el sector privado para concluir con un caso real de aplicación, en nuestro caso para el sector energético.

El tercero de los capítulos “Blockchain en la Gestión Pública” desarrolla diferentes usos de la cadena de bloques para las Administraciones Públicas, entre los que encontramos “Kleros” plataforma para la justicia descentralizada, “BenBen” plataforma para la gestión de tierras en distintos países, blockchain y su uso en la Autoridad Monetaria de Singapur y finalmente blockchain aplicado a los sistemas sanitarios.

Más tarde, el cuarto y penúltimo capítulo denominado “Blockchain en la Gestión del Sistema Democrático” explica como es la democracia actual de nuestro país y como puede ayudar o participar blockchain en ella, el segundo epígrafe habla de la aplicación real de la cadena de bloques en la comunidad autónoma de Cataluña y por último de la aplicación “TIVI” para el desarrollo en línea de sistemas de votación.

Para concluir, en el quinto y último capítulo de este TFG, incluimos las conclusiones generales de todo el trabajo pero centrándonos en comentar las referidas a los usos de la tecnología en las Administraciones Públicas, tema que es el objeto principal de dicho proyecto.

## 2. MARCO CONCEPTUAL

A lo largo de este capítulo seremos capaces de comprender en que consiste la tecnología de la cadena de bloques, desarrollando su funcionamiento y componentes básicos. De esta forma estaremos en condición de poder afrontar el desarrollo del resto del TFG, comenzando también en este capítulo por hablar de algunas de las utilidades que está aportando blockchain al sector privado, en que sectores se está apostando por esta tecnología con mayor énfasis, que empresas se han posicionado como punteras en el desarrollo de patentes relacionadas con la cadena de bloques y hablaremos por último del sector energético y como se prevé su futuro tras el desembarco de blockchain en él.

### 2.1 DEFINICIÓN DE BLOCKCHAIN

#### 2.1.1 INTRODUCCIÓN A BLOCKCHAIN

Seguro que todos hemos oído hablar en los últimos años de la tecnología *blockchain*, palabra muy nombrada en diversos ámbitos, pero cuyo significado y utilidad, poca gente llega a entender con claridad.

*Blockchain* se define como “un sistema de contabilidad distribuido digital que actúa como un registro abierto, compartido y de confianza que realiza transacciones entre las partes y no se almacena por una autoridad central y sigue manteniendo el enfoque tradicional”. (Berryhill, Bourgerly y Hanson 2018).

Esta tecnología surgió en la década de los años 90 pero como todos sabemos fue con *Bitcoin* cuando se produjo su expansión por todo el mundo. *Bitcoin* es una moneda virtual e intangible que nació en el año 2008-2009 tras la crisis de *Lehman Brothers*. Con *Bitcoin* se pretendía crear la posibilidad de realizar pagos electrónicos entre dos personas (Person to Person, P2P) sin la necesidad de un intermediario que verificara la operación y a la vez permitiendo asegurar a los usuarios que no iban a sufrir robos o fraudes. Esto es posible gracias al sistema utilizado por esta criptomoneda, que no es otro que *Blockchain* que funciona utilizando una red distribuida de ordenadores y algoritmos criptográficos convirtiéndose en un sistema encriptado que proporciona a sus usuarios seguridad y protección de sus datos y de las transacciones o movimientos que realicen a través de este sistema.

El *Bitcoin* nació con la idea de ser una red incensurable y por lo tanto completamente pública, que incluso se preparó para funcionar con cierto número de usuarios “deshonestos”. Frente a estas redes públicas, surgen las redes permisionadas, un paso intermedio entre los sistemas centralizados que tenemos en la actualidad y en los que todo el proceso es realizado en una localización central, a través de terminales o computadoras conectadas todas ellas a una computadora central en la que se confía el cien por cien del trabajo y las redes públicas incensurables. Estas redes “permisionadas” funcionan a través de la existencia de unos usuarios de confianza que son los que certifican las transacciones y dan permiso al resto de actores que quiere acceder.

A pesar de esto, tanto en las redes permisionadas como en las que no lo sean, todos los nodos tienen que certificar las transacciones que se producen y lo que difiere de unas redes

a otras, son los protocolos de consenso utilizados por estas. (Corporation, Aplicaciones del blockchain en el sector público 2018)

Para hacernos una idea de su funcionamiento, hemos de pensar que es parecido al de un libro mayor de contabilidad utilizado por cualquier empresa, pero cuyos apuntes son públicos y descentralizados. Cualquier transacción que se realice a través de *Blockchain* es transmitida y registrada por todos los nodos o integrantes de la red, lo que permite que todos los participantes tengan toda la información permanentemente actualizada. Por ello es necesario que para que se produzca un cambio por ejemplo de propiedad de un bien, este sea aceptado por el resto de usuarios y registrado como un nuevo nodo.

Es aquí donde nace la utilidad de la tecnología blockchain ya que si todos dicen que algo ha pasado, acabamos creyendo que es verdad y confiando en esa información, creando así un sistema seguro para cualquier tipo de transacción.

Cada operación genera un registro denominado "Token" y cada cierto número de "Tokens" u operaciones, se integra un bloque el cual va enlazado al anterior y al posterior, sin poder separarse.

Como vamos a ver a lo largo de este trabajo, la mayoría de *Blockchains* son sistemas descentralizados y distribuidos, lo que quiere decir que no hay una autoridad central capaz de alterar los contenidos de una cadena de bloques o capaz de controlar, aprobar o desaprobar transacciones tan sólo por su criterio, sino que hay que llegar a un acuerdo entre las muchas partes que lo conforman. Esta es una de las características principales de la tecnología Blockchain, que no puede borrarse ni repetirse lo que ya ha sido registrado, conociéndose como "inmutabilidad" de *Blockchain*. (CRIPTONOCIAS s.f.)

La criptografía de la cadena de bloques tiene la responsabilidad de generar un mecanismo para el cifrado seguro de las reglas del protocolo que rigen el sistema. Esta criptografía es además fundamental para evitar la manipulación por los distintos miembros que participan en la red, el hurto o incluso la posible introducción errónea de información en dicha blockchain, así como la responsable de generar firmas e identidades digitales cifradas.

A continuación se definen varios elementos básicos que componen las blockchains:

- **Nodo:** puede ser desde un ordenador personal hasta y según la complejidad de la red, un supercomputador. Con independencia de la capacidad de cómputo que tenga cada nodo, cada uno de ellos deben poseer el mismo software/ protocolo para poder comunicarse entre sí. Si esto no se cumpliera no podrían conectarse los distintos nodos entre sí y por lo tanto formar parte de la misma red de blockchain sería imposible.
- **Protocolo:** a través del protocolo que use una cadena de bloques se otorga un estándar común para hacer posible la comunicación entre los ordenadores/nodos que participen en la red, es decir, posibilitar un conjunto de reglas formales para la interacción de los distintos nodos. Existen protocolos muy conocidos como el TCP/IP o el SMTP.

- **Red P2P:** se trata de una red de computadoras que funcionan sin necesidad de contar ni con clientes ni con servidores fijos, lo que le otorga una flexibilidad que de otro modo sería imposible de conseguir. En esta red las distintas computadoras conectadas actúan al mismo tiempo como clientes y servidores con respecto a las demás computadoras conectadas.
- **Sistema descentralizado:** a diferencia de los sistemas centralizados donde toda la información está controlada por una única entidad, en las redes descentralizadas como ya comentamos con anterioridad, todos los ordenadores conectados tienen el mismo “poder” para hacer y deshacer dentro de la red, porque no hay una jerarquía entre los nodos, todos son iguales.

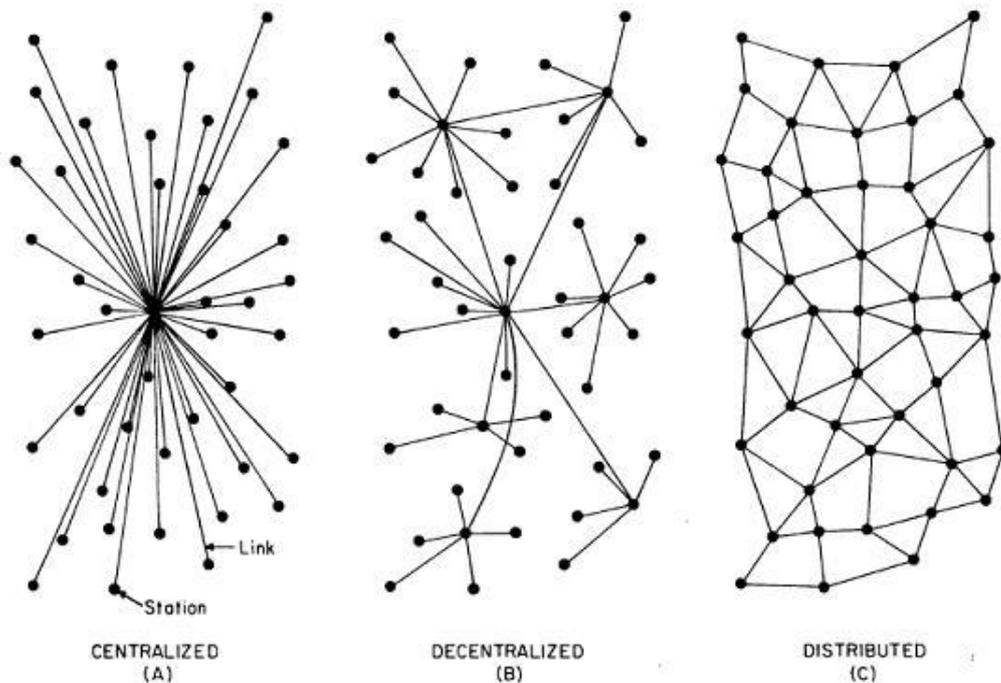
En la actualidad si se quiere modificar una transacción ya realizada, se debe realizar todo el proceso pero al revés, es decir, si se ha transferido una propiedad de una persona a otra y este traspaso ha sido autorizado por el sistema, será necesario realizar otra transferencia pero a la inversa para volver al estado inicial en el que nos encontrábamos con respecto a esta propiedad, porque lo que se ha realizado no se puede eliminar, es lo que antes nombrábamos y explicábamos como “inmutabilidad” de blockchain y que se considera una de las características básicas y más valiosas de estas redes.

Es la red de nodos la encargada de certificar que los datos referidos a esa transacción son los correctos, el consenso entre estos es una parte imprescindible de blockchain. Este consenso se sustenta en el protocolo que use la cadena de bloques que como hemos dicho es común para todos y sirve para verificar y confirmar las transacciones realizadas y asegurar la irreversibilidad o inmutabilidad de las mismas. De la misma forma, este consenso debe proporcionar a todos los usuarios una copia inalterable y actualizada de todas las operaciones realizadas en la cadena de bloques. Gracias a esto, aunque blockchain genere múltiples cadenas de bloques, siempre será legitimada la cadena de bloques más larga porque es donde se podrán encontrar todas las operaciones realizadas.

Gracias a que todos los participantes tienen una copia actualizada de la cadena y a que el sistema es distribuido, si se produjera la caída de alguno de los participantes o nodos, la información nunca se perdería o el servicio nunca dejaría de funcionar porque la información no la posee un solo nodo nunca.

Sin embargo, a la vez que esta tecnología se potencia y aparecen nuevos usos para ella, también están naciendo iniciativas para crear blockchains que puedan ser alterados por un administrador, aunque haya copias repartidas por distintas partes. Por ello, la tecnología blockchain es siempre distribuida, pero en estos casos pierde la característica de ser descentralizada. (CRIPTONOCIAS s.f.)

Figura 1- Representación visual de las redes comentadas.



Fuente: [academy.bit2me](http://academy.bit2me)

Las primeras Blockchains fueron diseñadas para ser:

- **Públicas:** cualquier persona sin ser usuario puede acceder y consultar las transacciones realizadas.
- **Abiertas:** cualquier persona puede convertirse en usuario y participar del protocolo común si posee unos mínimos conocimientos técnicos.
- **Descentralizadas:** lo son en cuanto que no existe un nodo que tenga más poder dentro de la red que el resto y debido a que por lo tanto todos son iguales entre sí a nivel de especificación de tecnología (esto no quiere decir que no existan nodos que tengan mayor o menor capacidad de cómputo que otros debido a sus características computacionales).
- **Pseudoanónimas:** los propietarios de transacciones no son identificables personalmente, pero sus direcciones sí son rastreables debido a su carácter público. Por eso, la mayoría de blockchains no pueden ser anónimas, excepto aquellas creadas o diseñadas expresamente para serlo.

A pesar de ello la propia tecnología blockchain ofrece la posibilidad de crear una cadena de bloques privada, cerrada y con participantes identificados:

- **Privadas:** no todos los datos inscritos en la blockchain tienen una difusión pública y solo los participantes o usuarios pueden acceder y consultar todas o algunas de las transacciones que se realicen.
- **Cerradas:** sólo se puede adquirir la condición de usuario o registrador de las transacciones si hemos sido invitados a participar en la red. En este sentido, el protocolo predeterminado podrá incluir distintos niveles de acceso a los

# Blockchain: Aplicaciones a la Administración Pública

usuarios, de modo que unos pueden tener la capacidad de registrar información y otros tener vetada esta opción.

- **Distribuidas:** el número de nodos que conformen la cadena de bloques privada puede estar limitado al número de participantes o a cierto número de ellos. En cualquier caso, todos estos nodos saben de la existencia del resto.

En la siguiente figura podemos ver de una manera visual y más ágil algunas de las diferencias o características que tienen o no algunas de las cadenas de bloques más famosas de la actualidad:

Figura 2. Diferencias entre blockchain públicas y privadas

	Públicos Bitcoin, Ethereum, Litecoin	Privados Hyperledger, Corda, Quorum	Federados Hyperledger, Corda, Quorum	Blockchain as a Service IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	≈	≈	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart Contracts	✓	✓	✓	NA
Existe recompensa por minado de bloques	≈	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	≈	NA
Seguridad basada en protocolos de consenso	✓	✗	≈	NA
Seguridad basada en funciones hash	✓	≈	≈	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Sí    ✗ No    ≈ A veces    NA No Aplica

Fuente: Elaborado por Allende y Colina (2018)

La fortaleza de una blockchain se basa en la cantidad de nodos que la protejan y en los incentivos que éstos puedan recibir por cumplir ese papel. La existencia de un mayor número de nodos operativos consigue que la posibilidad de sufrir ataques descienda. En las redes

públicas se mantiene la seguridad gracias a la voluntad de dichos participantes, y en las redes privadas cuyo acceso está limitado a previa invitación y a pesar de tener diferencias con las públicas, los participantes también desempeñan un rol en el mantenimiento de la cadena de bloques de una forma descentralizada.

Una vez hemos desarrollado la tecnología *Blockchain* podemos comenzar a comprender que esta haya llegado a ser tan nombrada y debatida en los últimos años y hayan aparecido tantos posibles ámbitos donde desarrollarla. Es por ello que muchos gobiernos están empezando a explorarla, para conseguir desarrollar nuevas soluciones a los problemas con los que se enfrenta la ciudadanía y sus gobiernos o simplemente para facilitar el proceso de muchas de las actividades cotidianas de las Administraciones Públicas (en adelante AAPP).

Tras los avances tecnológicos y la evolución de la sociedad, cada vez se reclama mayor participación, transparencia y cooperación entre las distintas partes que la componen, para que en las actividades que desarrollen las AAPP y el Estado, puedan participar de forma activa todos los ciudadanos.

A lo largo de la historia, se han repetido casos de fraude, abusos contra el ciudadano, etc. Esto ha llevado a la sociedad a estar mucho más atenta a todos los aspectos que le competen y afectan de forma directa o indirecta, y es por ello que *blockchain* puede ofrecer tantas posibilidades al trabajo realizado por las AAPP. Con el uso de esta tecnología se espera poder reducir los casos de estafa, corrupción y falsificación de datos por parte del ser humano en procesos públicos, tan frecuentes en nuestros días. (García Mateo 2018)

Durante estos años, los desarrollos tecnológicos de *blockchain* han sido más extensos en el sector financiero, pero a pesar de ello, la tecnología *blockchain* está emergiendo de forma asombrosa en el sector público. Los gobiernos están desarrollando acciones para aprender más sobre la tecnología y para introducir sus conceptos en sus actividades.

De forma rápida podemos nombrar la creación de una mesa redonda sobre *blockchain* en el Parlamento de la UE, la exploración por el Senado y la Asamblea Nacional de Francia, el reconocimiento como medio para la transferencia de bonos financieros por el Ministerio de Economía francés en el caso del capital privado... en total se cuentan al menos 200 iniciativas sobre *blockchain* en las que los gobiernos están involucradas. (Berryhill, Bourgerly y Hanson 2018)

## 2.1.2 FUNCIONAMIENTO DE BLOCKCHAIN

Antes de comenzar con la explicación propiamente dicha, debemos aclarar que dentro del entorno *blockchain*, la palabra transacción se refiere a cualquier intercambio de información susceptible de ser contenida en un bloque.

1. **Acceso a la red:** para ser parte de una red tenemos dos opciones dependiendo del tipo de *blockchain* que queramos utilizar, la primera consiste en descargar la aplicación correspondiente lo que nos convertiría en un nodo con los mismos derechos que el resto y la segunda acceder vía una interfaz web creada por los nodos administradores para el resto de usuarios autorizados. La primera de las opciones se da en las redes públicas, donde todo el que quiera puede acceder como un nodo más simplemente

descargando el software correspondiente y automáticamente se actualizará a la copia más reciente de la cadena de bloques. La segunda opción sin embargo se corresponde con las redes permisionadas donde como ya dijimos con anterioridad, existen unos nodos privilegiados que administran la cadena y deciden quien accede y quien no a la red. (Allende López 2018)

- 2. Registro de una transacción:** cuando un nodo quiere realizar una transacción, le tiene que enviar la información acerca de ese movimiento a todos los nodos con los que esté conectado. Aquí es donde aparece un primer protocolo en el que los nodos tienen que verificar que las transacciones que reciben sean válidas y una vez hayan verificado esto, ya podrán añadir esa transacción a su lista, denominada en blockchain “pool” reenviándola de nuevo a todos los nodos con los que estén conectados, continuando el proceso hasta que un nodo ignora la información porque ya la tienen registrada en su pool. (Allende López 2018)
- 3. Formación de un bloque:** cada ciertos segundos o minutos dependiendo del volumen de transacciones, se producen rondas, donde se escoge aleatoriamente a un nodo en cada una de estas para que cree un bloque. Este proceso es de los más importantes en *blockchain* y se conoce como protocolo de consenso. Este protocolo elige al nodo de forma aleatoria, y su función es la de crear con la versión actual de la cadena, un nuevo bloque que agrupe las transacciones que se han registrado en su pool desde la creación del último bloque. Una vez ha creado el bloque, envía esta nueva copia a todos los nodos con los que esté conectado y estos a su vez harán lo mismo, al igual que hacían con los movimientos individuales. El tamaño de cada uno de estos bloques es limitado y dependerá del tipo de *blockchain* en el que nos encontremos. (Allende López 2018)
- 4. Hash válido:** debemos tener en cuenta que el bloque creado por el nodo elegido en el protocolo de consenso, deberá tener un hash válido (código alfanumérico obtenido a partir de toda la información del bloque). Este hash es uno de los sistemas de seguridad que utiliza *blockchain*. Con la comprobación del resto de nodos de que este hash es válido, estos ya se encuentran en disposición de actualizar la cadena a la nueva versión que ya contendrá el nuevo bloque creado. (Allende López 2018)

### 2.1.3 PROTOCOLOS DE CONSENSO

Este protocolo como adelantamos anteriormente, es el utilizado para elegir al nodo que se encarga de proponer un nuevo bloque y a través del cual se llega a un consenso único entre todas las partes del sistema. Normalmente la elección del encargado de generar ese nuevo bloque es aleatoria, aunque hemos de decir que no todos los actores del *blockchain* tienen la misma probabilidad de ser elegidos.

A través de la elección aleatoria se intenta como es normal en *blockchain* que ninguno de los participantes pueda llegar a tener el control del sistema, cosa que ocurriría si fuese siempre la misma persona la encargada de proponer los nuevos bloques. Aun así existe la posibilidad de que los participantes que tengan más que ganar si el *blockchain* funciona de

manera adecuada, tengas más posibilidades de ser los elegidos en ese “sorteo”. (Allende López 2018)

Para que los participantes más interesados en ser los elegidos demuestren ese interés, se miden básicamente dos aspectos:

- Exigir a las entidades y a las personas que realicen algún tipo de esfuerzo por ser ellas las elegidas y recompensar al ganador normalmente en forma de criptomoneda.
- La segunda forma es, distribuir las probabilidades de ganar el sorteo proporcionalmente al número de activos, propiedades o bienes en la red de cada participante. (Allende López 2018)

A continuación, describimos algunos de los protocolos de consenso más utilizados:

- **Proof-of-Work (prueba de trabajo)**

Este protocolo de consenso fue diseñado para *blockchain* públicas y fue introducido por Satoshi Nakamoto en Bitcoin, para luego ser adaptado por otras muchas criptomonedas.

Corresponde al grupo de protocolos que exige un esfuerzo a los participantes para que logren ser ellos el elegido en proponer el siguiente bloque, dándose como hemos dicho anteriormente, una recompensa al ganador. Aquí los mineros ponen sus ordenadores a trabajar en resolver un acertijo criptográfico, teniendo más posibilidades de resolver el acertijo quien posea una computadora con mayor capacidad de cómputo. (Español 2018)

Al proceso de resolver el acertijo o encontrar el *hash* se le conoce como minar y es por ello que a las personas que participan en estos procesos, se les conoce como mineros.

Como encontrar el *hash* requiere gastar dinero y no se tiene certeza de que vayas a ser el primero en encontrarlo, parece improbable que un nodo maligno malgaste energía y dinero en intentarlo, porque aún ganando la prueba, a la hora de proponer un bloque falso o erróneo, el resto de nodos no lo aceptarían y por tanto se quedaría sin la recompensa y sin recuperar los recursos gastados.

En cambio, para motivar a los mineros honestos en resolver el acertijo, se ofrece una recompensa en forma de criptomoneda para el primer nodo que los resuelva. Por ejemplo en el caso de Bitcoin la recompensa es de 12.5 bitcoins, que equivalen a más de 125.000€ en la actualidad.

Sin embargo, este método también tiene inconvenientes como son la gran cantidad de energía que se consume, debido a la capacidad de cómputo necesaria, por lo que es un protocolo costoso e intensivo en energía. Según el MIT Technology Review, “Se estima que Bitcoin consume casi tanta energía anual como toda Nigeria o Perú, con un consumo que ronda los 39TWh al año”. Otro de los inconvenientes es que sólo se puede utilizar para blockchains asociados a criptomonedas, debido a que la recompensa es en forma de moneda virtual. (Allende López 2018)

- **Proof-of-Stake (prueba de participación)**

Este tipo de protocolo fue diseñado como alternativa a la prueba de trabajo, intentando corregir las desventajas de las que antes hablábamos, en especial el alto consumo de energía.

Al igual que Proof-of-Work, también fue diseñado para *blockchains* públicas, la diferencia entre este método y el anterior, es que este se basa en asignar mayor probabilidad de ganar el sorteo a los participantes que más activos posean dentro de la red *blockchain*.

Mientras que en “proof-of-work” a los mineros se les incentivaba a participar en beneficio de la red porque en caso de no ser así la energía que hubieran consumida sería desperdiciada porque como ya hemos comentado el bloque inválido que intentaran proponer sería rechazado por el resto de nodos, en este tipo de protocolo de “proof-of-stake” para poder participar, los validadores bloquean sus fondos y actuar contra la red puede llegar a significar que pierdan esos activos o fondos bloqueados.

Entre las ventajas que posee se encuentran, una mayor eficiencia al consumir menor energía, mayor velocidad al conseguir un procesamiento más rápido de las transacciones y que a su vez no requiere de una computadora tan potente como en la prueba de trabajo. (Allende López 2018)

Tras estos dos protocolos de consenso podemos encontrar “Leased-Proof-of-Stake” cuya diferencia con el anterior es que los participantes con pocos fondos pueden llegar a ceder sus probabilidades o “votos” de ganar el sorteo a otros. “Delegated-Proof-of-Stake” en la que los nodos pueden proponer a otros como sus elegidos para ser quienes formen el nuevo bloque, sería una especie de elección democrática. Y “Proof-of-Importance” que funciona como la prueba de trabajo pero dando mayores probabilidades de ser elegido en función de la actividad que tengan en la red en vez de en su dinero. (Allende López 2018)

Todas estas, son variaciones de las dos primeras que son los protocolos más utilizados y por tanto los más importantes.

Por lo tanto, durante este Trabajo de Fin de Grado (TFG), estudiaremos y evaluaremos una serie de posibles aplicaciones de la tecnología *blockchain* para nuestras AAPP que sirvan como ya hemos adelantado para solucionar los problemas a los que actualmente nos enfrentamos y facilitar de este modo el trabajo y veracidad de estas actividades, consiguiendo una mayor confianza en nuestro sector público a la vez que se abaratan costes.

## 2.2 ETHEREUM

Ethereum es una plataforma blockchain global de código abierto que permite a los desarrolladores crear y formalizar aplicaciones descentralizadas, y la cual igual que otras blockchains, tiene su propia criptomoneda nativa llamada “Ether” (ETH), que sirve para intercambiar valor y realizar pagos por el uso de los recursos de la red. Esta plataforma que vamos a desarrollar en los siguientes párrafos, fue desarrollada por el ruso Vitalik Buterin en el

# Blockchain: Aplicaciones a la Administración Pública

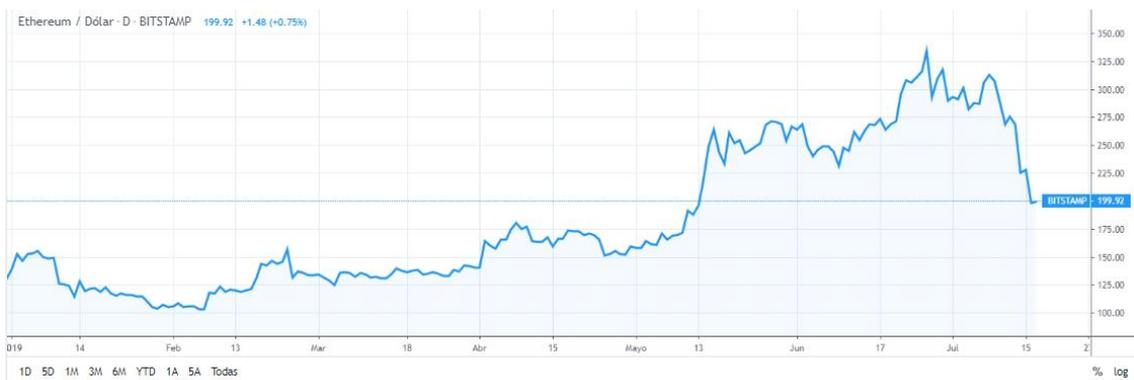
año 2014 y a diferencia del creador de Bitcoin el famoso Satoshi Nakamoto, Buterin es una persona física e identificable.

A pesar de que Ether sigue siendo considerada como la “hermana pequeña” de Bitcoin por el mero hecho de que Bitcoin es la más conocida, muchos inversores ya la consideran una criptomoneda con mucho más potencial que Bitcoin debido a que la creación de esta parece ser ilimitada mientras que la de Bitcoin tiene un límite de 21 millones de monedas en circulación.

Debemos tener en consideración que ambas monedas a pesar de utilizar blockchain, cuyo sistema parece fiable, siguen siendo criptomonedas sin regulación y vigilancia por parte de organismos oficiales y por lo tanto su cotización es extremadamente volátil, aspecto que es muy atractivo para muchos inversores, pero que a su vez es muy peligroso para nuestras inversiones en ellas.

En la siguiente gráfica podremos ver la evolución de la cotización de Ether desde comienzos de 2019 hasta mediados de Julio:

Figura 3. Cotización de Ether



Fuente: TradingView

Como ya adelantábamos antes y como podemos comprobar de forma visual, la cotización del Ether es bastante volátil llegando a pasar de los 150 dólares por Ether a prácticamente 350 dólares en tan solo un par de meses, es decir, un aumento de más del 100% para que pasados 30 días nos encontremos otra vez en el valor inicial, por ello puede ser una inversión muy atractiva para inversores a los que les atraiga el riesgo ya que pueden ganar mucho dinero gracias a estos cambios en la cotización, pero muy peligrosa para otros muchos inversores que tienen por naturaleza aversión al riesgo o simplemente que no son expertos en criptomonedas o en este tipo de inversiones y que pueden llegar a perder mucho.

Por lo tanto podemos ver como la inversión en estos activos es arriesgada debido a su gran volatilidad que puede hacernos ganar mucho dinero pero también perderlo todo. Estas grandes variaciones no suelen ser tan pronunciadas en valores de empresas o activos controlados por organismos oficiales ya que todo está mucho más regulado e incluso se puede llegar a cerrar una sesión si se están produciendo variaciones de importancia muy significativa.

# Blockchain: Aplicaciones a la Administración Pública

En la siguiente tabla, podemos ver como las criptomonedas más usadas de todo el mundo sufren variaciones de gran importancia en su valor en apenas unos meses, este es uno de los riesgos que entrañan pero que no exime del gran potencial que tiene la tecnología que hay detrás de ellas, es decir, blockchain.

Tabla 1.- Volatilidad de las 4 criptomonedas más conocidas del momento

VOLATILIDAD DE LAS CRIPTOMONEDAS MÁS CONOCIDAS			VARIACIÓN RELATIVA	VARIACIÓN
BITCOIN	01/03/2019	09/08/2019	161días	
	3.354,87 €	10.747,49 €	220,355%	7.392,62 €
ETHER (ETHEREUM)	26/01/2019	27/06/2019	152días	
	77,91 €	183,90 €	136,042%	105,99 €
LITECOIN	23/01/2019	21/06/2019	149días	
	31,76 €	138,52 €	336,146%	106,76 €
RIPPLE	24/02/2019	25/06/2019	121días	
	0,30 €	0,47 €	56,667%	0,17 €

Fuente: Elaboración propia

Volviendo al tema que nos ocupa que no es otro que entender Ethereum desde el punto de vista del blockchain, hemos de decir que la gran diferencia de Ethereum con otras blockchains como la comentada Bitcoin, es que esta nos permite crear nuevos tipos de aplicaciones en función de nuestras demandas conocidas como Dapps, mientras que Bitcoin sólo nos ofrece una aplicación particular de la tecnología de bloques para mantener un seguimiento de su moneda, los “bitcoins”.

Ethereum consigue esto a partir de una blockchain con un lenguaje de programación “Turing-completo”, que permite a cualquier persona con unos conocimientos mínimos en informática programar Smart contracts y aplicaciones descentralizadas que no pueden ser censurados y que son accesibles a todo el mundo. (Jimenez 2018)

Otra de las características importantes de Ethereum es que utiliza el protocolo de consenso Proof-of-Work usando el algoritmo Ethash que se creó por y para esta plataforma. Aunque esta característica podría cambiar en el corto plazo con el lanzamiento de Ethereum 2.0 del que los expertos comentan que llevará consigo una criptomoneda que use el protocolo Proof-of-Stake explicado con anterioridad.

Entre las aplicaciones que ya se han desarrollado y que se están usando a día de hoy, podemos destacar programas del tipo de:

- Aplicaciones financieras que permiten tomar prestado, prestar o invertir sus activos digitales.
- Juegos donde posees activos dentro del juego valorados en Ether y que luego pueden convertirse en ganancias en dinero real.
- Monederos de criptomoneda que nos permiten realizar pagos baratos e instantáneos con la moneda de Ethereum el ETH u otros activos.

- Mercados descentralizados, que nos permiten intercambiar activos digitales e incluso hacer e intercambiar predicciones sobre algunos de los eventos del mundo real.
- Etc.

## 2.2.1 SMART CONTRACTS

A través de los contratos inteligentes, es decir, los famosos “Smart contracts” se pueden crear en Ethereum las aplicaciones descentralizadas que hemos comentado, capaces de registrar transacciones de cualquier tipo de activos: inmobiliarios, monetarios, etc.

Pero, ¿qué es un contrato inteligente?

Este tipo de contratos se basan en “scripts” es decir, códigos informáticos que establecen comandos y sentencias que una vez se han ejecutado, hacen que el contrato se cumpla de manera autónoma y automática, sin la necesidad de que intervenga intermediarios ni otros participantes que alargan el proceso y aumentan el coste del mismo.

Por lo tanto, se establecen una serie de condiciones o acciones que una vez se han cumplido permiten que automáticamente el contrato se haga efectivo sin necesidad de que intervenga ninguna otra parte en el asunto. Por ejemplo, vamos a imaginar que nos encontramos apostan bitcoins a quien será el próximo ganador de Le Tour de Francia, y cada uno de los amigos apuesta por su favorito 2 bitcoins que depositaremos en una cuenta neutral controlada por el contrato inteligente. Una vez haya finalizado la prestigiosa carrera ciclista, el Smart contracts conectará con algún sitio de noticias deportivas fiable para verificar quien ha sido el campeón de Le Tour y de forma autónoma se depositarán los bitcoins en la cuenta del amigo acertante.

Con este proceso no se ha necesitado la firma de ningún profesional verificando que el contrato se ha cumplido y se ha hecho eficaz de forma correcta, ahorrándonos dinero y tiempo como antes comentábamos.

A su vez, este tipo de contratos pueden ser creados por personas y empresas pero también por máquinas o tecnología artificial que funcionen de manera autónoma y tienen validez sin necesidad de estar controlados por una autoridad oficial gracias a su naturaleza de origen que no es otra que blockchain que les aporta carácter descentralizado, inmutable y transparente.

La primera vez que se habló acerca de los Smart contracts, fue allá por el año 1995 en un documento hecho público por el jurista y criptógrafo Nick Szabo, que dos años más tarde en 1997 complementaría con otro documento mucho más desarrollado sobre estos contratos inteligentes. El problema fue que aunque se tenía la idea, era imposible llevarla a cabo debido a que la tecnología no era lo suficientemente potente y desarrollada como para tener un sistema financiero digital repartido a lo largo de todo el mundo que pudiera soportar estos contratos.

No fue hasta el nacimiento de Bitcoin y de su tecnología, blockchain, cuando este tipo de contratos comenzaron a hacerse realidad, ya que Bitcoin contiene Smart contracts que se

# Blockchain: Aplicaciones a la Administración Pública

ejecutan automáticamente y por defecto cuando los usuarios de la red hacen movimientos. (Academy by Bit2me s.f.)

En la siguiente tabla, podemos observar algunas de las diferencias que existen entre los contratos tradicionales elaborados a mano por profesionales y los contratos inteligentes.

Tabla 2.- Contrato tradicional vs Smart Contract

CONTRATO TRADICIONAL	SMART CONTRACTS
Pago manual	Pago automático
Tarde de 1-3 días	Automático
Mayor coste	Coste fraccionado, más barato
Presencia física	Presencia virtual
Necesidad de intermediarios (Notarios, abogados, etc)	No es necesaria la intervención de intermediarios
Es necesario depositar los fondos del contrato	No es necesario el fideicomiso de los fondos

**Fuente: Elaboración propia**

Entre los posibles contextos donde se pueden utilizar este tipo de contratos, podemos destacar algunos:

**Mercados distribuidos** que permiten implementar contratos P2P y trading en los mercados con criptomonedas postulándose como un competidor completo al sistema financiero actual.

**Propiedades** como automóviles, teléfonos, casas o elementos no físicos controlados a través de la cadena de bloques conforman las conocidas como “Smart property”. Al transformar una propiedad en una propiedad inteligente se consigue que se puedan intercambiar con una mayor confianza, ya que se reduce el fraude, las tarifas de mediación cobradas por los distintos profesionales independientes y además que se lleven a cabo operaciones que de otra manera nunca se hubieran realizado.

**Automatización** de herencias estableciendo la asignación de los activos o bienes tras el fallecimiento del propietario. Como ya hemos explicado el funcionamiento de un contrato inteligente, esto permitiría que en cuanto se produjera el fallecimiento de la persona propietaria, las condiciones del contrato se cumplirían y de forma automática y autónoma se ejecutaría repartiendo en este caso los fondos a las direcciones/personas establecidas en el contrato.

En las **empresas** se podría definir con un Smart Contract como se repartirá el dinero procedente los beneficios o las acciones en casos de ampliación... de esta forma, la sociedad garantiza que lo votada se ejecutará, teniendo una transparencia total y seguimiento de los movimientos realizados.

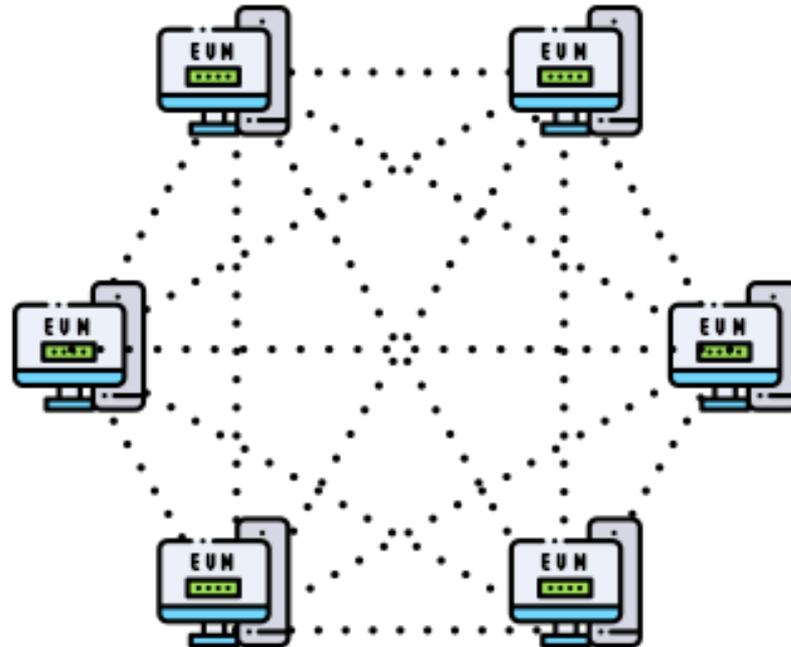
## 2.2.2 ETHEREUM VIRTUAL MACHINE

Se trata de un software que se centra en proporcionar seguridad a Ethereum evitando que un programador malicioso pueda atentar contra la seguridad de los nodos de la red o contra la propia seguridad de Ethereum. Además asegura que un programa no pueda tener

acceso ilícito a otros, permitiendo que se establezca una comunicación sin ninguna interferencia potencial.

Este Ethereum Virtual Machine está compuesto de una gran cantidad de ordenadores conectados entre sí a través de Internet que ejecutan los ya comentados Smart contracts.

Figura 4. Ordenadores conectados por Internet formando la Ethereum Virtual Machine



Fuente: VirtualForce

Paralelamente a cumplir con su función de seguridad en la red, la Ethereum Virtual Machine también busca simplificar el desarrollo y actualización de aplicaciones, permitiendo que se puedan ampliar las funciones de la red de una forma mucho más rápida y sencilla.

Gracias a este software se pueden realizar todas las funciones de Smart contracts que nos ofrece Ethereum.

### 2.2.3 GAS EN ETHEREUM

El Gas en la plataforma no es otra cosa que el coste o el valor que hay que pagar por realizar una o varias operaciones dentro de la red. Hablamos de operaciones desde una simple transacción hasta crear una aplicación descentralizada con la ayuda de Ethereum.

Al igual que en el mundo real, no todas las operaciones tienen el mismo coste dentro de la red. Por ejemplo una operación en la que tuviesen que intervenir más nodos para realizarla porque posee un número mayor de instrucciones, tendría un valor superior y por lo tanto un coste en gas superior que otra operación compuesta por menos instrucciones y por tanto más sencilla.

Una de las características de esta “unidad de gasto” de Ethereum, es que no sólo tiene un uso dentro de la red. A continuación vamos a enumerar los distintos usos que se le da al Gas en la plataforma:

- El primero de ellos como ya hemos comentado, es como medida para asignar un coste a la ejecución de las distintas tareas que dependiendo de la dificultad o incluso de la velocidad con la que queramos que se ejecuten esas tareas, el coste en gas será mayor o menor.
- Otra de las funciones que cumple el Gas en Ethereum es en la ayuda a mantener una red segura, limpia de información innecesaria y por lo tanto de colapsos. Esto es posible porque cuando se quiere realizar una operación como ya hemos dicho, hay que pagar por ella en Gas y por lo tanto este coste o comisión evita que se añadan operaciones que contenga información inútil a la blockchain a la vez que se evitan las instrucciones que ejecuten tareas repetitivas por códigos, las cuales podrían llegar a colapsar el sistema al repetirse infinitas veces.
- Por último, el trabajo de los mineros en la red se ve recompensado en forma de Gas que les sirve para “pagar” todos los recursos que han utilizado en su trabajo como pueden ser electricidad, tiempo, hardware... a la vez que se les ofrece una recompensa por el trabajo realizado.

Una vez hemos visto las funcionalidades del Gas, tenemos que dejar claro que este Gas no es una nueva criptomoneda, no sirve como unidad de cambio. Es decir, no podemos poseer una cantidad de gas determinada y decir que por ello tenemos cierto “dinero”, porque este Gas sólo existe dentro de la Ethereum Virtual Machine para determinar la cantidad de trabajo que se está realizando.

Por ello, cuando un minero recibe Gas por el trabajo realizado, tienen que “cobrarlo” y este proceso es algo complejo porque como hemos dicho esta unidad de gasto no es una moneda y por tanto no se puede cobrar.

Lo que hacen estos mineros es darle valor monetario a los recursos consumidos, y como nos encontramos en Ethereum este valor se da en Ether la moneda oficial de la red, por lo tanto podríamos decir que una cantidad de Gas tiene un precio equivalente en Ether para que los mineros puedan cobrar su recompensa en esa criptomoneda.

Un ejemplo de esta operación sería pensar que 500 unidades de Gas equivalen a 1 Ether y por lo tanto si una operación ha consumido 2000 unidades de Gas, el minero debería recibir como recompensa 4 Ether.

Se podría pensar que si al final el minero “cobra” en Ether porque no se mide todo directamente en Ether y ahorraríamos tener que medir en Gas y luego cambiar. Pero si pensamos que el valor del Ether como comentamos unos puntos atrás tiene un valor volátil, entonces todo cobra sentido.

Sería totalmente ineficiente medir el gasto transaccional y de procesos de Ethereum en Ether porque cada vez que cambiase el valor del Ether en el mercado habría que actualizar

el código de protocolo para ajustarlo a la realidad, proceso que evita la red al medir todo en Gas porque este se mantiene constante según unos parámetros.

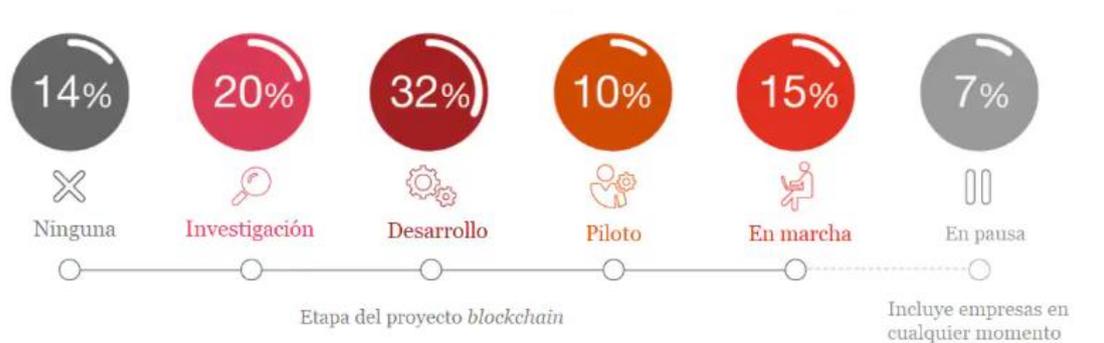
Esta característica permite al sistema poseer una mayor estabilidad por no tener que crear un mercado paralelo entorno al Gas. (Ethereum 2018)

## 2.3 BLOCKCHAIN Y EL SECTOR PRIVADO

Antes de comenzar con el análisis de las posibles aplicaciones de *blockchain* en las AAPP, debemos tener en cuenta que esta tecnología también ha tenido un impacto importante en el sector privado, ya que permite a las industrias que la emplean abaratar costes en muchos de sus procedimientos y conseguir este abaratamiento de forma mucho más rápida. Además, su uso en el área de la ciberseguridad está cobrando cada vez mayor protagonismo.

Un informe de la compañía *PwC España* realizado sobre 600 ejecutivos de las grandes empresas internacionales revela que cuatro de cada cinco directivos ya tienen en marcha en sus respectivas compañías proyectos con el nombre de *blockchain*. (PwC España 2018)

Figura 5. Grado de desarrollo de aplicaciones blockchain en empresas privadas



Fuente: PwC Global Blockchain survey, 2018

En esta imagen extraída del informe publicado por PwC podemos ver como el desarrollo, investigación, puesta en marcha..., de aplicaciones *blockchain* en las empresas privadas se está generalizando, y ya son sólo aproximadamente el 14% de las empresas estudiadas (multinacionales) las que no muestran ningún tipo de interés por esta nueva tecnología.

Este informe ha revelado que estas grandes compañías entienden los beneficios que les puede aportar la tecnología *blockchain* y no quieren perder la oportunidad de poder explotarlos y mucho menos de que sus competidoras les superen por no haber sabido aprovecharse de ella.

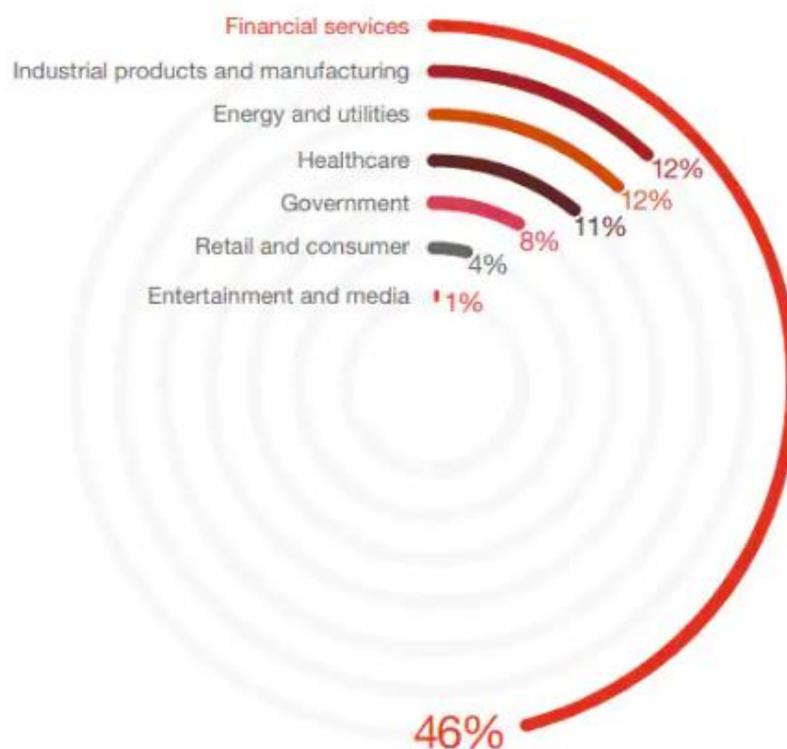
Por ello estos directivos esperan que aproximadamente entre el 10% y el 20% de la economía mundial este gestionada en mayor o menor medida por *blockchain* para el año

# Blockchain: Aplicaciones a la Administración Pública

2030, siendo el sector financiero donde mayor sea su utilización. Aunque también podamos destacar otros muchos sectores donde su aplicación va a ser importante como la energía, salud, consumo, entretenimiento, industria y el sector público que será del que hablaremos más adelante. (PwC España 2018)

En la siguiente imagen podemos ver de forma visual cuales son los sectores donde más empresas están apostando por *blockchain* y por lo tanto donde la tecnología se está desarrollando con mayor rapidez y adquiriendo un papel más importante:

Figura 6. Sectores que lideran el desarrollo de blockchain



Fuente: PwC Global Blockchain survey, 2016

Como ya hemos comentado, es el sector financiero donde mayor es la inversión en el estudio y desarrollo de tecnologías y plataformas que utilicen o basen su funcionamiento en blockchain, seguido por el sector industrial, energía, salud... La diferencia es muy importante entre el sector de las finanzas y el resto ya que casi la mitad de las inversiones en esta tecnología son de empresas relacionadas con banca, servicios financieros, etc.

En el caso de la salud, blockchain puede tener gran importancia en el desarrollo de aplicaciones para la atención médica, ya que puede ayudar a reducir las pérdidas de tiempo en el día a día las cuales son tan frecuentes. Se podrá recoger en la misma plataforma y gracias a este sistema toda la información sobre los estados de los pacientes y llevar un registro histórico de los mismos.

Otro de los sectores donde blockchain puede introducir mejoras importantes es en transportes y logística, donde puede mejorar en gran medida los flujos de información a lo

largo de los distintos procesos. Se trata de un sector con gran complejidad lo que favorece que tecnologías como la que tratamos puedan introducirse con gran aceptación ya que pueden ayudar en la automatización de procesos, la reducción de los distintos trámites administrativos, gubernamentales y aduaneros y como es de esperar en la reducción de actividades fraudulentas.

Estados Unidos, China y Australia quizás sean los países más avanzados en esta tecnología y por lo tanto los que están liderando su desarrollo, esto podemos verlo en el uso que están haciendo grandes compañías de estos países de *blockchain*, donde entre otros podemos destacar:

- **Banco Industrial y Comercial de China (ICBC):** esta institución ha comenzado a utilizar *blockchain* para autenticar certificados digitales y almacenar sus datos, todo con el objetivo de aumentar la eficiencia en la emisión de certificados y evitar que los usuarios llenen varias veces los mismo documentos.
- **JP Morgan y Berkshire Hathaway:** en el caso de estas dos grandes compañías estadounidenses, encontramos que sus CEOs no son fanáticos ni mucho menos de Bitcoin. Warren Buffett aseguró que “las monedas digitales se podrían comparar con veneno para ratas”. Sin embargo, ambos saben que la tecnología *blockchain* es otra historia, y ya han comenzado a utilizarla para desarrollar distintas funciones en sus conglomerados mejorando el proceso de gestión y seguimiento de datos de sus operaciones diarias.
- **Walmart:** el gigante minorista se ha unido con IBM para la implementación de *blockchain* en su negocio, consiguiendo un seguimiento de los productos cárnicos y avícolas vendidos en sus distintos establecimientos. Gracias a la tecnología la multinacional es capaz de rastrear la información desde el agricultor hasta el consumidor final, pasando por distribuidores y minoristas.

La necesidad de la compañía por implementar estos servicios nació a raíz del brote de salmonella en uno de sus productos concretamente en el melón fresco el cual tuvieron que retirar del mercado y ante la cual la compañía tuvo dificultades para rastrear donde estaba el epicentro del problema debido a la escasez y complicada documentación que se poseía.

- **Maersk:** otra de las multinacionales que se ha asociado con el gigante de la tecnología IBM para trabajar con *blockchain* es Maersk la naviera más grande del mundo. El objetivo era el desarrollo de la primera plataforma que monitoreara el envío de carga a través de *blockchain*.

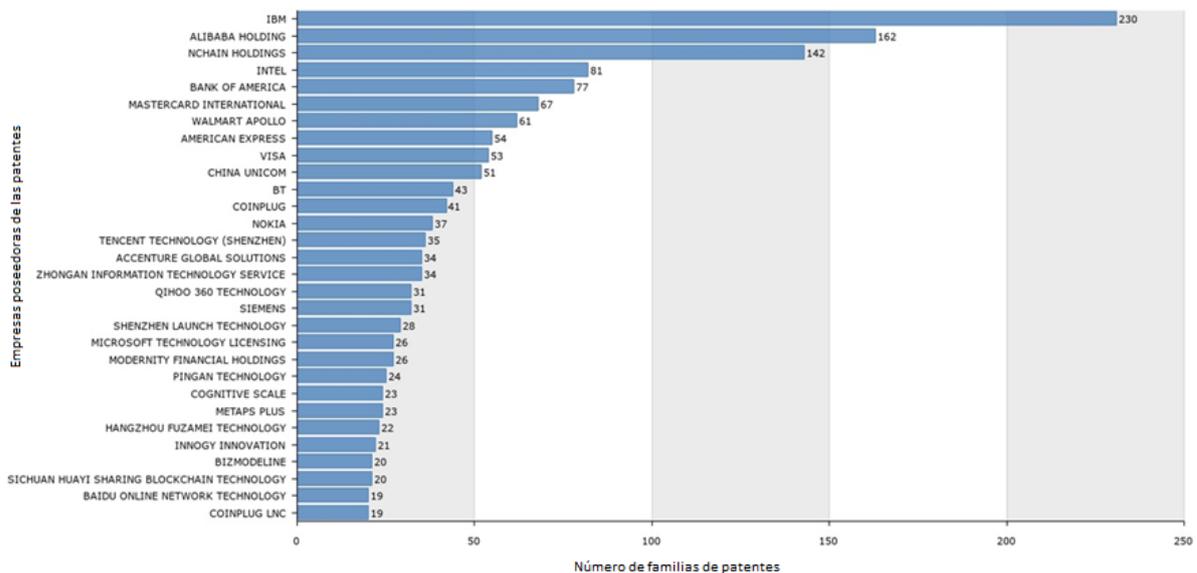
Tradelens ha sido el resultado de esta asociación, consiguiendo una plataforma capaz de registrar los detalles del envío de carga desde que un envío sale de un área hasta que llega a su destino.

Toda la información necesaria para las distintas partes involucradas en estas cadenas de suministros se encuentran ahora dentro de la plataforma, por lo que como dicen desde el gigante naviero, “la implementación de *blockchain* tiene el potencial de simplificar y mejorar la seguridad cuando se trata de envío internacionales”.

En la siguiente gráfica podemos observar cuáles son las compañías internacionales que mayor número de patentes relacionadas con *blockchain* poseen en la actualidad y así podemos

saber que sectores y que empresas son las que más están apostando por esta tecnología a esperas de que triunfen muchos de estos proyectos por los que están invirtiendo.

Figura 7.- Multinationales con mayor número de patentes de blockchain en su poder



Fuente: Marc Kaufman para Blockchain Patent Chronicle

La empresa con mayor número de patentes relacionadas con la tecnología de la cadena de bloques en la actualidad es la multinacional estadounidense IBM (International Business Machines Corporation) la cual es una de las empresas de tecnología y consultoría más importantes de todo el globo terrestre y de la que hablaremos a lo largo del TFG por estar o haber participado en diversos proyectos que vamos a estudiar durante los siguientes epígrafes.

Las compañías que siguen a la estadounidense IBM en número de patentes son Alibaba Holding que es una multinacional china dedicada al comercio electrónico en Internet, NChain Holdings que es una de las líderes mundiales en asesoramiento, investigación y desarrollo de todo tipo de tecnologías que integren la cadena de bloques y la estadounidense Intel Corporation conocida por ser el mayor fabricante de circuitos integrados de todo el mundo, circuitos que son utilizados prácticamente para todos los dispositivos electrónicos que utilizamos hoy en día como ordenadores y teléfonos móviles.

Estos usos los podemos extrapolar prácticamente a la mayoría de las grandes firmas a nivel mundial, y debemos de pensar que el uso de *blockchain* por las compañías más potentes no es una mera casualidad, sino la señal de que el presente y el futuro quizás pasen por *blockchain* y ninguna de estas empresas se lo quiere perder.

### 2.3.1 INTERNET DE LAS COSAS

El concepto que todos conocemos como “internet de las cosas” se entiende como la conexión de internet con los objetos cotidianos de nuestro día a día en vez de con las personas. En la actualidad aún está por desarrollarse en su mayoría, ya que debería de

codificar unos 50 a 100.000 millones de objetos porque de media una persona tiene a su alrededor e “interactúa” con aproximadamente 1000 a 5000 objetos.

Por ejemplo, con el internet de las cosas libros, neveras, lámparas, alimentos... estarían conectados a internet y todos ellos equipados con dispositivos de identificación, permitiendo que los stock fueran mucho más reducidos y las medicinas, alimentos y demás productos no corrieran el riesgo de estar caducados, podríamos saber la localización exacta de cada objeto que poseamos y por lo tanto evitar la pérdida de los mismos, etc.

Aunque hoy en día esa realidad aún parece lejana, muchas de las grandes compañías tecnológicas apuestan a un gran desarrollo en los próximos años, permitiendo que nuestras prendas de vestir, electrodomésticos del hogar, vehículos, envases... estén conectados a internet y puedan enviar y recibir información.

Actualmente gracias a esto, tenemos dispositivos que nos permiten encender y apagar la calefacción desde el móvil, vigilar el interior de nuestras casas o negocios, graduar la luz de una casa, etc. En un futuro reciente se espera tener incluso una nevera capaz de detectar que alimentos han caducado o cuáles se han agotado y ella misma se encargará de contactar con el supermercado para encargar todo lo necesario.

Pero a la vez que las ventajas para nosotros como consumidores de estos objetos se presentan infinitas ayudándonos enormemente en nuestro día a día, también existen inconvenientes y el más importante como cualquier dispositivo conectado a internet no es otro que la seguridad, la posibilidad de ser hackeados. Hoy en día, podemos leer en la prensa constantes noticias sobre si “Alexa” de Amazon o “Google Home”, dos de los asistentes de voz más vendidos del mercado graban y guardan las conversaciones entre las personas del hogar, las canciones que escuchamos, las preguntas que les hacemos... Según las compañías esto sólo es para mejorar los servicios que el producto nos ofrece, pero con tal cantidad de información almacenada sobre nuestras vidas y la posible falta de seguridad se crea cierta alarma social.

Por ello, gran parte de los fabricantes de este tipo de productos conectados a internet se han puesto a buscar soluciones y blockchain es clara candidata por ser una opción bastante interesante.

Un grupo de empresas formado por **Bosch, Bank of New York Mellon, Cisco, Foxconn Technology Group, Gemalto** y las startups especializadas en blockchain **Consesus Systems, BitSE y Chronicled**, han anunciado el nacimiento de un consorcio para el desarrollo de blockchain en el internet de las cosas. (FinTech 2017)

A través de esta unión, este grupo de empresas busca desarrollar un protocolo de la cadena de bloques específico para el internet de las cosas, con el objetivo de mejorar los servicios ofrecidos y obviamente ampliar la seguridad de los mismos.

En este caso, hemos podido ver como empresas privadas se están uniendo para desarrollar mucho más la tecnología blockchain y poder explotarla donde los usuarios la demanda, y uno de los puntos donde una empresa puede obtener ventaja competitiva frente a sus competidoras no es otro que la seguridad frente a ataques en internet de los productos/servicios que ofrezca.

En el siguiente epígrafe de nuestro trabajo, ya pasamos a valorar distintas opciones o usos que se plantean desarrollar o ya están en marcha de blockchain con finalidades en el sector público, es decir, en las AAPP que son el objeto del Trabajo de Fin de Grado.

Gran cantidad de estas aplicaciones, a pesar de estar en uso nos iremos dando cuenta que les falta todavía desarrollarse y crecer, aspecto que es normal debido a que esta tecnología ha comenzado a explotarse con un mayor énfasis en los últimos años, pero a su vez seremos capaces de comprender el gran potencial que guarda la cadena de bloques para las AAPP y de esta forma poder hacernos una idea de cómo podrán ser muchos de los procesos cotidianos que desarrollemos con los gobiernos, instituciones públicas... de aquí a unos años.

## 2.4 TECNOLOGÍA BLOCKCHAIN Y LA INDUSTRIA ENERGÉTICA

A pesar de que uno de los inconvenientes de Bitcoin sin lugar a dudas es el enorme gasto de energía que supone su funcionamiento, ya es una realidad que la tecnología que sostiene a Bitcoin, es decir, blockchain, está siendo utilizada cada vez con mayor frecuencia por las compañías energéticas.

La cadena de bloques es considerada por muchos expertos como una posible revolución para el sector energético ya que puede ayudar a aspectos tan comunes como los cobros de las facturas de energía, la manera en que los productores que también son consumidores denominados como “prosumidores” interactúan con la red eléctrica, la compraventa de certificados energéticos..., consiguiendo que todos ellos se realicen de una manera más eficiente.

Hasta ahora, el uso de blockchain en este sector se ha visto limitado porque la tecnología no estaba preparada para soportar los grandes volúmenes de transacciones que se realizan cada segundo, y también ha afectado enormemente la no existencia de un marco regulatorio que pueda ayudar a estas aplicaciones a llegar a comercializarse.

A pesar de estos inconvenientes, se tiene la certeza de que es en el sector energético donde blockchain puede ofrecer un mayor número de ventajas debido al número de participantes que lo componen (distribuidores, productores, consumidores, proveedores, comercializadores...). La cadena de bloques permitiría la realización de las transacciones sin necesidad de terceros que aumenten los costes del proceso, también permitiría aumentar la conexión entre los mercados mayoristas y minorista y mejorar la seguridad de todos los datos tratados. Con estas mejoras se podría reducir por ejemplo el coste de nuestra factura de la luz debido al ahorro en costes de intermediarios y a la realización de los procesos de una manera más efectiva y eficiente, pero también cabe la posibilidad de que esto sólo sirva para aumentar el beneficio de las grandes empresas energéticas del mundo.

A continuación hablaremos de algunas de las posibles intrusiones que puede realizar la tecnología de blockchain en este sector tan importante en nuestros días.

## 2.4.1 POSIBLES APLICACIONES DE BLOCKCHAIN EN EL SECTOR ENERGÉTICO

Como comentaremos en el epígrafe “Cataluña y Blockchain”, la cadena de bloques tiene una reciente e importante aplicación debido al nacimiento de los denominados prosumidores o consumidores activos que generan su propia energía para su autoconsumo pero que pueden inyectar de nuevo en el mercado energético los excedentes que no sean capaces de gastar y hayan generado. Ahí es donde blockchain puede ayudar a mejorar el intercambio de esta energía entre vecinos, aspecto que trataremos. Además en este ámbito blockchain puede ayudar a reducir el cambio climático ya que permite una mejor distribución de energías limpias, potenciando su uso y la inversión en ellas.

Este intercambio de energía entre vecinos ya se logró en Brooklyn por la compañía *LO3 Energy*, que logró que los dueños de paneles solares de este barrio neoyorkino pudieran vender los excedentes que no utilizaran a sus vecinos a través de una plataforma que funcionaba con blockchain, recibiendo a cambio tokens representativos. Otro de los casos es el de compañía australiana *Power Ledger*, que ofrece a sus clientes ya desde su propia página web lo siguiente:

*“si tiene paneles solares en su azotea, puede usar nuestra plataforma para vender el exceso de energía a su vecino. Si tiene una batería de almacenamiento, puede almacenar su energía y venderla para maximizar sus ganancias de la energía solar que genere”*

Esta compañía permite a los usuarios establecer precios de compra y venta para el intercambio de estos excedentes a un precio justo establecido por la oferta y la demanda al igual que ocurre en otros muchos mercados como la bolsa de valores.

En esta línea encontramos al grupo suizo *Axpo* que ha desarrollado una plataforma basada en la cadena de bloques a través de la cual los operadores y propietarios regionales pueden vender directamente la electricidad a sus clientes finales sin la necesidad de intermediarios, energía que producen en plantas solares, eólicas, hidroeléctricas y de biomasa.

Gracias a blockchain también se espera poder mejorar el registro de todos los datos de las distintas transacciones y sus historiales de una forma incorruptible e inmutable. De este modo, se puede rastrear el flujo de las distintas energías que utilizamos desde su origen hasta que llega a nosotros como consumidores finales y comprobar de esta forma que se trata de fuentes de energías limpias y fiables o que se ajustan a lo establecido por las autoridades, etc. Por ejemplo en este sentido *Iberdrola* y *Megavatio Control* ambas empresas españolas, han desarrollado un software con funcionamiento a través de blockchain que permite certificar que una fuente de energía es limpia o no y su origen frente a los consumidores finales.

Al igual que ayuda a registrar de donde procede la energía para conocer su origen y desarrollo, puede ayudar a registrar las emisiones contaminantes de las distintas fuentes de energía y así ayudar a controlarlas con efectos positivos sobre el cambio climático.

Blockchain también está siendo utilizado por compañías petroleras de todo el mundo para mejorar los procesos y eliminar de ellos los documentos de carga y otros tipos de formularios de registros que se necesitan para cada transacción y donde se invierte mucho

tiempo, a cambio, este tipo de formularios se pueden realizar con los ya explicados contratos inteligentes lo que genera una mayor eficiencia en este tipo de operaciones.

A esta revolución también se han subido empresas españolas del sector como Endesa, Gas Natural Fenosa e Iberdrola, uniéndose al proyecto Enerchain que permite a través de una plataforma descentralizada las transacciones de gas y electricidad entre dos empresas en cualquier zona de la Unión Europea y para cualquier periodo. En este proyecto desarrollado por la empresa de software alemana Ponton, están participando 39 empresas europeas de energía. Gracias a esta plataforma se consigue uno de los propósitos por los que se creó blockchain, que no es otro que el intercambio de información, datos, o cualquier elemento como en este caso energía entre dos partes, lo que denominábamos al principio del TFG como transferencias P2P. (Observatorio Blockchain 2019)

En la siguiente tabla podemos ver de forma más esquematizada los usos que hemos nombrado añadiendo también otros usos como la posible aplicación a los vehículos eléctricos y para la gestión de activos, facilitando entre otras cosas la transferencia de estos de un individuo a otro.

Tabla 3.- Posibles usos de blockchain en el Sector Energético

Categoría - Caso de uso	Descripción
Transacción de energía	La capacidad de los individuos y las comunidades para obtener e intercambiar energía de igual a igual y de máquina a máquina sin intermediarios (complejos) y con un control sin precedentes de sus propios datos y uso de energía, además de contar con la capacidad de obtener energía de fuentes más pequeñas, incluidos sus propios activos renovables.
Certificados de origen (Energías renovables)	La reinención completa de los complejos sistemas de contabilidad, transacciones e informes para aumentar la participación, simplificar el comercio y liquidar instantáneamente.
Vehículo conectado a la red (V2G)	Los individuos, las comunidades y las empresas utilizan los vehículos eléctricos para potenciar su propio suministro energético, pero también para recibir valor por proporcionar electricidad adicional de los vehículos a la red.
Participación local en nuevos mercados (flexibilidad, capacidad)	Los individuos y las comunidades actúan localmente proporcionando energía y almacenamiento (solar, almacenamiento, EV), realizando servicios como respuesta de la demanda y recibiendo valor del operador del sistema.
Gestión de activos y cadena de suministro	La capacidad de cambiar de proveedor instantáneamente, o la titularidad de activos, sin la complejidad de involucrar a múltiples partes, registros y procesos complejos.

Fuente: 20minutos.es

## 2.4.2 CONCLUSIONES

Tradicionalmente el sector de la energía se ha basado en la explotación masiva de petróleo, gas natural, carbón y la producción de otros productos energéticos como la electricidad. Actualmente y debido a la extrema necesidad ante el cambio climático, se debe y se está apostando por otro tipo de energías menos contaminantes, lo que se denomina como energías renovables, estas son las energías que provienen de recursos naturales que no se agotan y a los que podemos recurrir de manera permanente para su generación. Estas energías provienen de plantas fotovoltaicas, eólicas, geotérmica, maremotriz, de la biomasa, etc. Ante estas numerosas fuentes de energía y todos los procesos que se necesitan para su desarrollo y gestión hasta el consumidor final hemos podido comprobar que la cadena de bloques podría ayudar a mejorar el desarrollo de muchos de estos procesos.

Después de explorar algunas de las opciones que ofrece blockchain a uno de los sectores que más dinero mueve en todo el mundo, debemos preguntarnos si de verdad esta tecnología será capaz de transformarlo.

Parece estar claro que el sector está sufriendo transformaciones gracias a la llegada de esta tecnología, y que las diferentes empresas que lo componen están apostando por ella confiando en que puede aportarles numerosas ventajas. Esto lo hemos visto con los números ejemplos redactados con anterioridad y podemos decir que el sector energético está cambiando, nos estamos moviendo hacia la eliminación o reducción de las energías no renovables y la digitalización del sector. Hoy en día existen más de 300 proyectos sobre el campo de blockchain/energía y son numerosas las empresas interesadas en tratar de optimizar sus procesos con la ayuda de la cadena de bloques.

Sin lugar a dudas blockchain desprende infinidad de ventajas, pero también supone ciertos riesgos y uno de los más importantes como ya comentábamos y que ha frenado el desarrollo de la tecnología en el sector es la falta de regulación o la falta de normativa sobre la tecnología. Desde nuestro punto de vista es necesaria la existencia de una regulación correcta y unificada por parte de organismos oficiales para que se produzcan transformaciones tan importantes en cualquier sector que nos rodea y por lo tanto en el sector energético también. Las empresas necesitan un marco regulatorio de confianza que guíe sus actuaciones sobre esta tecnología y que les garantice que todo lo que inviertan en ella no va a ser en vano y pueda llegar a ser inútil en el futuro por diversos aspectos.

Finalmente pensamos que blockchain crecerá transformando al sector energético, ya que hemos podido ver algunas de las formas en las que puede ayudar a reducir los procesos, eliminar intermediarios, facilitar la introducción de las energías renovables, etc. Ahora falta ver si los ahorros económicos que se supone que blockchain traerá consigo, se verán reflejados en las facturas de los consumidores finales ofreciéndoles energías con menores precios que los actuales o si simplemente ayudaran a las grandes compañías petroleras, eléctricas... a aumentar sus márgenes y beneficios mientras el precio de la energía se mantiene o crece para el consumidor de a pie.

## 3. BLOCKCHAIN EN LA GESTIÓN PÚBLICA

### 3.1 PROYECTOS BLOCKCHAIN EN LAS AAPP

Hasta ahora hemos podido desarrollar y entender en gran medida que es blockchain, en que se basa y como funciona a la vez que observábamos que puede revolucionar sectores como el financiero permitiendo realizar transacciones seguras sin necesidad de que participen intermediarios que verifiquen y aseguren estos movimientos. Pero el potencial de blockchain no se limita al sector financiero y en los siguientes epígrafes vamos a ver diferentes usos que benefician tanto a la AAPP como prestadora de los servicios como a los destinatarios, en estos casos la ciudadanía.

Blockchain puede ofrecer multitud de posibilidades a las AAPP, algunas de estas ya están en desarrollo o incluso funcionando en algunos países, pero otras muchas están por explorar y desarrollar.

Estas funcionalidades las podemos clasificar desde el punto de vista de las funciones o características inherentes de las cadenas de bloques. Por ejemplo, blockchain puede ser interesante para aspectos relacionados con los registros públicos y privados, registros de propiedad, padrones de vivienda y población, registros educativos, sanitarios, de justicia, etc.

Por otro lado, al igual que hemos desarrollado el internet de las cosas y hemos hablado de empresas privadas que están comenzando a realizar consorcios para trabajar en ello, si nos fijamos en la AAPP, este internet de las cosas también es muy interesante para el crecimiento de las ciudades conectadas. Gracias a blockchain y al big data se podrían generar importantes oportunidades en aspectos como la gestión de mobiliarios de las ciudades, parques, agua, electricidad y demás servicios que son responsabilidad de la AAPP y que podrían realizarse de manera más eficiente con servicios conectados que informaran en todo momento del estado por ejemplo de las instalaciones y servicios.

Para el desarrollo de todas estas opciones se necesita obviamente de la colaboración de las distintas AAPP y que apuesten por esta tecnología invirtiendo en ella. A lo largo de este TFG podremos ver como cada vez son más las opciones que aparecen y por tanto las instituciones que se fijan en esta tecnología como posible instrumento para mejorar sus servicios y veremos usos de la tecnología para aspectos tan importantes para las instituciones públicas como son la justicia, sanidad, registro de propiedades y sistemas de votación entre otros.

### 3.2 BLOCKCHAIN Y LA JUSTICIA DESCENTRALIZADA

#### 3.2.1 JUSTICIA EN LAS PRIMERAS SOCIEDADES

Desde las primeras civilizaciones como la griega ya se aplica la justicia, pero de una manera muy diferente a la que conocemos en el actualidad, era la llamada “justicia entre pares” caracterizada porque no había abogados, jueces... que aplicasen sus conocimientos sobre la leyes a la hora de juzgar, sino que se hacía entre personas normales con el mismo nivel de conocimientos que se presentaban en el tribunal el día del juicio porque querían

formar parte del jurado y donde se desarrollaba un sofisticado proceso de selección para elegir que ciudadanos formarían parte del jurado de ese juicio.

En estas sociedades griegas llegaron a la conclusión de que la justicia podía funcionar entre pares siempre y cuando se cumplieran tres condiciones que no son otras que:

- El jurado debía recibir remuneración.
- El jurado debía ser voluntario.
- La selección del jurado debía realizarse siempre por sorteo.

### 3.2.2 KLEROS, JUSTICIA DESCENTRALIZADA.

Las sociedades han ido avanzando y en la actualidad con la llegada de internet y la globalización nos encontramos con problemas que obviamente hace unos años no existían, pero que han devuelto a la actualidad las ideas entonces utilizadas por la sociedad griega. Las personas trabajan en muchos casos como autónomos independientes para otras personas, empresas, etc., de cualquier parte del mundo y esto conlleva innumerables ventajas pero también ciertos inconvenientes que hay que solventar.

A su vez las compras y transacciones en línea entre personas de todo el mundo han aumentado de forma exponencial y entre el 3 y el 5% de estas transacciones termina en disputas, lo que significa más de 700 millones sólo en 2015. Los métodos de justicia existentes para este tipo de problemas son demasiado lentos y costosos sobre todo cuando hablamos de cantidades de dinero no demasiado elevadas, por ello el nacimiento de la justicia descentralizada es un importante avance hacia el futuro. (Corporation, Kleros, un Protocolo de Justicia para Internet 2017)

Por ejemplo imaginemos que trabajamos como autónomos en nuestro país, es decir, en España y contactamos con un programador informático de Argentina para que nos realice una página web a través de la que realizar nuestro trabajo o a través de la cual nuestros clientes puedan contactar con nosotros.

Cuando el programador termina su trabajo nos entrega el producto y a nosotros que nos encontramos en la otra parte del mundo no nos gusta y decidimos que lo hagan de nuevo, a lo que nos responden desde Argentina que quieren el pago de este primer sitio web antes de realizar de nuevo la página web y entonces entramos en una disputa. Imaginemos que el coste de este sitio web habría sido de 250€ y obviamente no podemos ir a un juicio tradicional a Argentina por 250€ porque es totalmente ineficaz.

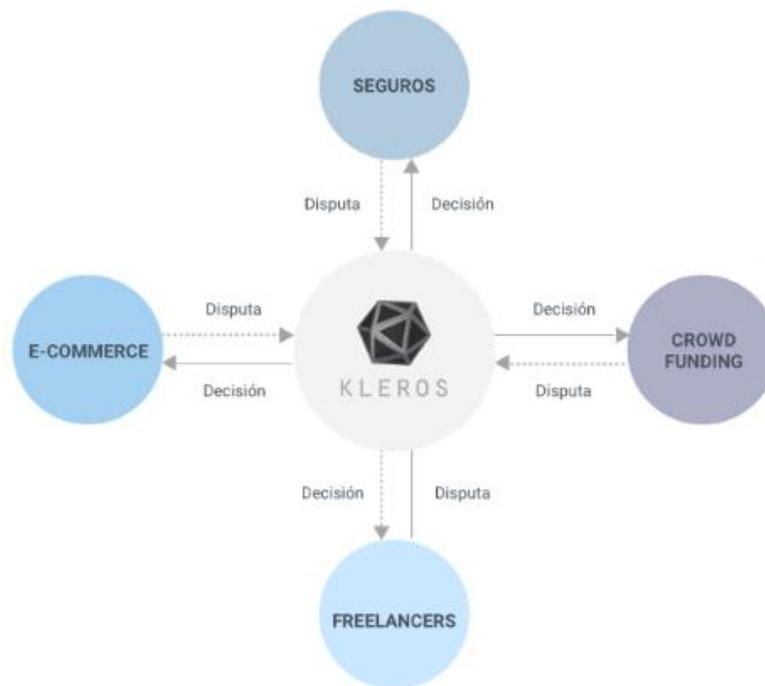
En la actualidad este tipo de disputas por pequeñas cantidades entre personas de distintos países son cada vez más comunes y en muchos de los casos no tienen solución o es muy complicada para el montante del que se trata.

¿Cómo podríamos solucionar esto con Blockchain? Pues ahí es donde aparece "Kleros", denominado por sus creadores como el protocolo de resolución de conflictos en blockchain.

Siguiendo con nuestro ejemplo, en vez de pagarle nosotros directamente al programador argentino, lo que haríamos sería poner el dinero en un Smart Contracts donde el dinero quedaría bloqueado ahí hasta que se realizara el trabajo y donde el programador puede ver que su dinero estará disponible en cuanto finalice el encargo. La diferencia es que entre ambas partes acordamos que en caso de disputa habrá un árbitro y ese árbitro no es otro que Kleros.

Cuando se produce esta disputa, entonces Kleros es quien elige un jurado de expertos sobre el tema, estos expertos serán quienes decidan quien de las dos partes lleva razón según lo establecido en el contrato y el producto o servicio que se entregó con posterioridad. Cuando determinen quien lleva la razón el dinero se transfiere a su cuenta y el jurado recibe un dinero por parte de la persona o empresa que perdió el juicio. Este tribunal se forma a partir de jurados dispuestos a colaborar.

Figura 8- Kleros como red de adjudicación descentralizada



Fuente: Medium Corporation, 2017.

A parte del caso comentado, con esta aplicación de *blockchain* podemos resolver otros muchos problemas como por ejemplo casos de conflictos en juegos en línea que tanto está creciendo en los últimos años, comentarios desafortunados en las redes sociales, financiación no utilizada en el caso de un producto que nunca llega a materializarse tras haber sido financiado y por lo tanto los inversores tienen derecho a recuperar su dinero de la manera más efectiva posible, etc. (Ast 2019)

Para hacernos una idea del posible uso de este tipo de justicia descentralizada, tenemos que valorar que el comercio electrónico se espera que alcance un mercado de 2 billones de dólares para el año próximo, que la economía colaborativa alcance un valor de 335

mil millones de dólares para dentro de 5 años y que el crowdfunding utilizado para la compra de acciones alcance un mercado de 96 mil millones de dólares anuales solo en los países en desarrollo. (Corporation, Kleros, un Protocolo de Justicia para Internet 2017)

Con este sistema, las AAPP podrían resolver de forma mucho más rápida las disputas que tienen con los contribuyentes por temas como subvenciones, ayudas, pagos de impuestos, etc. Y sobre todo con personas que no sean de nuestro país y tengan cualquier tipo de deber con las AAPP españolas.

### 3.2.3 CONCLUSIONES

Una vez explicado el funcionamiento de la justicia descentralizada, podemos entender de su importancia y utilidad a día de hoy y en un futuro, con multitud de aplicaciones donde poder ayudarse de esta aplicación de *blockchain*. Se trata de un sistema rápido y fiable según los creadores, donde no tendremos problemas de seguridad, filtración de nuestros datos o sobornos a la vez que ofrece privacidad a los usuarios gracias al equipo que dirige sus experimentos criptoeconómicos que aseguran un protocolo lo más seguro posible.

Asumiendo que en internet podremos estar más o menos a salvo de los hackers pero nunca 100% seguros frente a ellos, y que en la sociedad de nuestros días es prácticamente imposible trabajar o vivir sin acceso a internet o sin realizar algún trámite a través del mismo, podemos llegar a la conclusión de que la idea es buena y que posiblemente con el paso del tiempo se perfeccione mucho más para pulir los pequeños errores que pueda tener.

Yo como usuario quizás prefiera si no fuera por el tiempo que se tarda, la justicia tradicional simplemente por el hecho de que quien determina mi culpabilidad o no, es una jueza o un juez expertos en el tema, y en el caso de Kleros no conozco quien es el jurado, ni sus aptitudes, ni sus conocimientos, ni nada sobre él, entonces eso puede crear mucha desconfianza sobre las conclusiones que de sus disputas se obtenga. Pero bueno básicamente en eso se basa *blockchain*, en algo que dicen muchos al final pasamos a pensar que es la verdad.

Como conclusión creo que la justicia descentralizada pasara a tener mucha más repercusión en los próximos años, sobre todo para temas donde no merezca la pena pasar por la justicia tradicional ya sea por la poca importancia del tema, porque el dinero que se debe o nos deben no es lo suficientemente importante para nosotros..., aspectos que nos conviene que se resuelvan de forma rápida y por los cuales no nos merece la pena meternos en papeleos extras.

## 3.3 BENBEN A TRAVÉS DE BLOCKCHAIN

### 3.3.1 DESARROLLO DE BenBen

BenBen es una empresa privada fundada en 2014 por Emmanuel Noah (CEO) y Daniel Block (ex-COO) y formada en la actualidad por un equipo de 4 ingenieros que se propusieron mejorar la tecnología gubernamental en Ghana.

La función de la empresa es proporcionar un registro digital administrado por Ethereum de todos los registros de tierras existentes en Ghana, con la misión de digitalizar el ecosistema del mercado inmobiliario en África y reducir hasta la eliminación los problemas relacionados con las transacciones financieras terrestres en el continente. (Noah 2018)

En particular con esta plataforma se abordan dos problemas relacionados con el registro de tierras en el país africano:

En primer lugar la difícil determinación de forma legal de parcelas y títulos de propiedad de la tierra, por la falta de un seguimiento adecuado y sistemático, y la ausencia de almacenamiento de información digital que impide a las autoridades y propietarios tener certeza sobre la titularidad de las tierras en el país.

El segundo de los problemas, es la falta de una relación abierta entre los dueños de las tierras, las agencias gubernamentales del país como es la Comisión de Tierras de Ghana y las instituciones financieras, para facilitar las actuaciones entre ellos. Ya que hasta la llegada de BenBen era necesario ir físicamente a la Comisión de Tierras para buscar los registros existentes en papel y entonces llevarlos a la entidad financiera, lo que como podemos entender es un proceso demasiado lento e ineficiente en el siglo XXI.

El registro de tierras centralizado del país africano es en papel y además no permite garantizar los derechos de propiedad en Ghana ya que el sistema de registro en papel no es exigible en los tribunales. Como consecuencia de esto, los bancos no aceptan prácticamente ninguno de estos registros como garantía a la hora de pedir préstamos por parte de la población lo que les deja sin financiación y además, no pueden confiar en que esas tierras sean tomadas por otros. (Berryhill, Bourgerly y Hanson 2018)

BenBen como ya hemos dicho proporciona un registro digital administrado por Ethereum de todos los registros de tierras del país. A través de una combinación de satélites es capaz de certificar la información terrestre. Agrega toda la información y de este modo las instituciones financieras y La Comisión de Tierras tienen acceso en tiempo real a todos los datos disponibles.

De esta forma es mucho más sencillo certificar la propiedad de una tierra en el caso por ejemplo de querer realizar su venta, acceder a un crédito o demostrar simplemente que la propiedad le corresponde a la persona en concreto.

Otro de los aspectos en los que puede ayudar es en el caso de las disputas por la propiedad de la tierra, ya que al tratarse de un registro digitalizado e inmutable, sirve a los tribunales como base fiable a la hora de actuar como testigo en un juicio. Hay que tener en cuenta que aproximadamente el 70% de las disputas judiciales en Ghana están relacionadas con la propiedad de la tierra, de ahí la importancia de esta aplicación de *Blockchain*.

Actualmente aún está en proceso de asentamiento y crecimiento, pero desde 2017 cuentan con más de 10.000 registros integrados en sus bases de datos, y cuentan también con el apoyo de las instituciones públicas y privadas por su seguridad y utilidad. Además, se ha conseguido reducir el tiempo en confirmar la propiedad de la tierra de un año hasta tres meses

con el uso de BenBen y el tiempo en recibir información en tiempo real de la Comisión de Tierras se ha reducido también de un mes a los tres días. (Berryhill, Bourgerly y Hanson 2018)

En la siguiente tabla podemos ver las mejoras que se han producido en algunos de los procesos de la administración de Ghana referentes a la propiedad de las tierras gracias a la aparición y uso de BenBen:

Tabla 4.- Reducción en los tiempos de espera gracias a BenBen

	SIN EL USO DE BENBEN	CON EL USO DE BENBEN
TIEMPO PARA CONFIRMACIÓN DE LA PROPIEDAD DE LA TIERRA	1 AÑO	3 MESES
TIEMPO PARA RECIBIR INFORMACIÓN DE LA COMISIÓN DE TIERRAS DE GHANA	1 MES	3 DÍAS

**Fuente:** Elaboración propia

En los próximos años, desde BenBen esperan poder aumentar su financiación y el número de miembros que trabajan en la plataforma para de este modo conseguir expandirse a varios países de África como son Botsuana, Nigeria y Costa de Marfil, para seguir con su proyecto que no es otro que ser reconocidos como la principal solución existente en África para la construcción de mercados inmobiliarios digitalizados y ayudar a asentar las bases para asegurar la inversión, crecimiento y desarrollo basándose en las ricas tierras del continente africano.

### 3.3.2 CONCLUSIONES

Como hemos podido ver BenBen es una plataforma con gran futuro ya que soluciona problemas muy habituales en los países en los que opera y por lo tanto la ciudadanía y las AAPP la deben de entender como un medio para conseguir un tratamientos de las propiedades de tierras justo en esos países que por su condición de subdesarrollados hasta la fecha no se estaba dando.

La gran ventaja competitiva de esta aplicación frente a otras que están y surgirán en el mismo mercado objetivo, es que aparte de ser la primera en fijar sus objetivos en este ámbito, aspecto que le da mucha ventaja frente a sus competidores, es que desde BenBen están realizando su crecimiento de la mano de los principales actores del sector público y privado en el mercado de tierras de esos países.

Creer mediante el apoyo de gobiernos e instituciones públicos te garantiza que tus usuarios verán en tu empresa a un grupo de profesionales en los que confiar para tratar sus distintos problemas y por lo tanto esto conseguirá que se tenga una confianza extra en ella

frente a nuevos competidores que nazcan e intenten introducir sus negocios en el sector desde cero.

Por otro lado, desde mi punto de vista el crecimiento en el resto de países de África también es posible, ya que estos pueden ver los resultados positivos que está teniendo en su país vecino como es Ghana y ello conllevará a que el resto de actores quieran trabajar con ellos.

Sin embargo, si por ejemplo pensamos en un crecimiento de BenBen a países desarrollados como los europeos o EEUU, entonces esa implantación la veo más complicada, debido a que en estos países las disputas por temas de tierras son mucho menores y estos problemas ya están solucionados por nuestras administraciones públicas. A pesar de esto, pienso que una idea como la de BenBen que está consiguiendo tener un registro digital administrado por blockchain de esta problemática, sí que puede servir como ejemplo para mejorar los servicios públicos de prácticamente todos los países en este ámbito, porque se trata de una tecnología novedosa y porque siempre se puede mejorar.

### **3.4 BLOCKCHAIN Y LA AUTORIDAD MONETARIA DE SINGAPUR**

La Autoridad Monetaria de Singapur (MAS, por sus siglas en inglés) y el resto de instituciones financieras del país asiático son reconocidas por su eficiencia y constantes innovaciones en el sector. Una vez más han demostrado que esta consideración no es por casualidad y la Autoridad Monetaria del País comenzó a explorar el potencial y los posibles beneficios que se podrían extraer de la contabilidad distribuida y blockchain en lo que respecta a aplicaciones financieras y bancarias.

Desde Singapur se realizó un estudio que desprendió datos relativos a la ineficiencia y lentitud de los pagos interbancarios y de las distintas transacciones financieras transfronterizas dentro del país.

El 16 de noviembre de 2016 esta Autoridad anunció un convenio con R3, una empresa de tecnología blockchain y un grupo de instituciones financieras formado por algunas tan conocidas como “Bank of América”, “Citi” y “Credit Suisse” para el desarrollo de un proyecto de prueba que consiguiera realizar pagos interbancarios utilizando tecnología blockchain.

Este proyecto fue nombrado como “Proyecto Ubin” y la Mas declaró: “El proyecto desarrollará un sistema piloto en el que se utilizará la infraestructura de Blockchain para emitir y transferir fondos entre los participantes”.

Como hemos podido ver constantemente a lo largo del trabajo, la tecnología blockchain tiene la capacidad de permitir procesos y transacciones más transparentes, resilientes y a un menor coste que los procesos tradicionales donde como ya hemos dicho infinitud de veces, los numerosos intermediarios y procesos burocráticos ralentizan el ritmo de las operaciones y añaden costes al proceso. Por ello la Autoridad Monetaria de Singapur apostó por blockchain y los libros de registro digitalizados y descentralizados para llevar a cabo este proyecto, con el objetivo de evaluar las posibles implicaciones de actuar con un DLT o blockchain y sus beneficios para el ecosistema financiero de Singapur.

Antes de continuar con el proyecto en sí, debemos comentar que a menudo los términos “DLT” o tecnologías de registro distribuido y “blockchain” son utilizados con el mismo significado. Y es que como ha pasado con muchos otros productos o servicios, el éxito de estos supera al término que lo abarca y acaba conociéndose a todos los productos por el nombre de la marca. Pero de la misma forma que no todas las hojas adhesivas son Post-It, no todas las DLT son “blockchain”.

Por lo tanto para hacernos una idea, tenemos que pensar que DLT es simplemente una base de datos que gestionan varios participantes y no está centralizada, es decir, no existe una autoridad central que ejerza su poder frente al resto de participantes. Mientras que blockchain es un tipo de DLT con un conjunto de características particulares. (BBVA 2018)

El proyecto ha utilizado a Ethereum como soporte para el funcionamiento de su red, consiguiendo encriptar la moneda nacional y diferenciándola de otras formas digitalizadas de pago mantenidas por el Banco Central por medio del nombre de “SGD-on-ledger”.

Para el desarrollo del proyecto se han dividido las acciones en tres fases, la fase 1 sirvió de base para evaluar la viabilidad e implicaciones de DLT, y para identificar los elementos necesarios para posibles futuras mejoras. Deloitte se encargó de realizar la investigación y un estudio de factibilidad sobre las aplicaciones potenciales de la tecnología explorando los siguientes aspectos:

- Optimización de liquidaciones de pagos entre bancos locales participantes.
- Beneficios y dificultades de “crear” una criptomoneda de la moneda del banco central de país.
- Pasos para habilitar transacciones transfronterizas.
- Métodos efectivos de digitalización de pagos.

Ya en 2017, se comenzó a desarrollar la fase dos, donde ya comenzaron a participar el conjunto de instituciones financieras que se habían involucrado a participar en el proyecto, y donde se desarrolló con éxito un prototipo de software de tres modelos diferentes para realizar pagos descentralizados y liquidaciones interbancarias con mecanismos de ahorro de liquidez. En esta fase participaron las siguientes instituciones financieras:

- Citi
- Credit Suisse
- Bank of America Merrill Lynch
- DBS Bank Ltd
- HSBC Limited
- J.P. Morgan
- Mitsubishi UFJ Financial Group
- OCBC Bank
- Singapore Exchange
- Standard Chartered Bank
- United Overseas Bank

También participaron los siguientes socios tecnológicos desarrollando cada uno de ellos unas funciones dentro del proyecto:

- Accenture: gestionar y desarrollar prototipos
- R3: Soporte en la plataforma Corda DLT
- IBM: Soporte en la plataforma Hyperledger Fabric DLT
- ConsenSys: Soporte en la plataforma Quorum DLT de J.P. Morgan, consiguiendo demostrar con éxito que un dólar virtual o tokenizado de Singapur podría funcionar como medio de liquidación interbancaria diaria.
- Microsoft: Implementación de prototipos en Azure Blockchain

Durante la fase 3 se siguió desarrollando los potenciales de una criptomoneda nacional y se continuó realizando pagos transfronterizos a través de la tecnología blockchain.

Finalmente, las futuras fases de este proyecto se centraran en desarrollar nuevos métodos para realizar pagos transfronterizos utilizando la moneda digital del banco central. (Pollock 2018)

A raíz de este proyecto se han desarrollado nuevas opciones, por ejemplo la conocida como **“Entrega versus pago (DvP)”** que comenzó a desarrollarse el 24 de Agosto de 2018 y cuyo objetivo era la liquidación de activos tokenizados en diferentes plataformas blockchain. Se pretendía que las instituciones financieras y los distintos inversores pudieran llevar a cabo el intercambio simultáneo y la liquidación final de estas monedas tokenizadas y de los valores, mejorando así la eficiencia del proceso y reduciendo los posibles riesgos en la liquidación.

En este proyecto participaron tres empresas (Anquan, Deloitte y Nasdaq) que aprovecharon el software del que hablábamos en la fase 2 del Proyecto Ubin, dándose por finalizada su colaboración en noviembre de ese mismo año cuando consiguieron demostrar que la liquidación DvP, la interoperabilidad entre intermediarios y la protección de los inversores se pueden lograr de forma conjunta con el uso de aplicaciones basadas en blockchain.

Otro de los casos más conocidos donde el proyecto sirvió de referencia es en Sudáfrica, donde el Banco de la Reserva de Sudáfrica (SARB) utilizó todo lo desarrollado en Singapur para darle forma a su “Proyecto Khokha”.

Al igual que la Autoridad Monetaria de Singapur con el Proyecto Ubin, el SARB se decantó por Quorum (una implementación empresarial de Ethereum) de J.P. Morgan para el desarrollo de su proyecto particular “Khokha”.

Este proyecto se lanzó con la idea de realizar una prueba de concepto para un sistema de pago basado en la cadena de bloques, fue en 2018 cuando se publicó el informe con algunos de los resultados. En este informe se indicaba que el volumen diario del sistema de pagos de Sudáfrica podía realizarse en un tiempo record de dos horas, y gracias al uso de blockchain las transacciones podrían ser totalmente confidenciales.

Todavía no se ha puesto en marcha el sistema basado en blockchain de manera oficial, pero sí que se ha logrado conseguir experiencia propia sobre las capacidades y oportunidades

que pueden ofrecer los libros de contabilidad distribuidos y sobre cómo podría mejorar el sistema de pagos sudafricano.

Este proyecto sudafricano logró ser reconocido

Como hemos podido ver a lo largo de este epígrafe, son numerosos los bancos centrales de distintos países los cuales han comenzado a hacer pruebas piloto con la tecnología blockchain obteniendo buenos resultados tras la aplicación de estos proyectos. Esto nos hace pensar que el futuro de blockchain en las AAPP está garantizado, pero todavía falta mucho por realizar.

La tecnología blockchain en el sector financiero y sobre todo en aspectos gubernamentales relacionados con la banca y la economía, puede ofrecer gracias a su inmutabilidad, una gran oportunidad para la lucha contra la corrupción y el lavado de dinero tan habitual en muchos países pero en especial en países como Sudáfrica y sus países vecinos del continente africano donde la lacra de la corrupción sigue minando el posible desarrollo de estos Estados.

## 3.5 BLOCKCHAIN EN EL SISTEMA SANITARIO

El sistema sanitario de un país es uno de los aspectos que quizás más importe a la ciudadanía de un territorio, una sanidad bien organizada, eficiente, de calidad y con un coste adecuado aporta tranquilidad y bienestar a los habitantes de una región.

En nuestro país, España, nos encontramos con uno de los sistemas sanitarios más eficientes del mundo según el índice que confecciona la agencia financiera Bloomberg. Este puesto en el ranking se ha conseguido gracias a poseer una de las esperanzas de vida más longevas del mundo y un coste relativo de la sanidad que se encuentra dentro de media.

Pero ¿podría mejorarse el sistema sanitario?

Seguro que sí, y una de las apuestas de mejora de la sanidad se encuentra en la utilización de blockchain. Hemos podido ver infinitud de áreas donde la cadena de bloques puede aportar ventajas gracias a sus características y esto nos lleva a pensar que en sanidad también puede aportar nuevas opciones.

En el sistema sanitario a menudo nos encontramos con que la información crítica de un paciente está dispersa por varios sistemas y a veces es difícil o se convierte en un proceso lento cuando algún experto necesita consultarla para realizar su trabajo de manera correcta. Esto ocurre porque muchas de las infraestructuras del sector público y por lo tanto las de sanidad también, no se encuentran preparadas para ofrecer un intercambio de información entre los distintos actores de manera eficiente. Aquí es donde blockchain tiene grandes cosas que ofrecer ya que puede transformar el acceso a la información sobre los pacientes.

Como hemos comentado en el párrafo anterior, el historial médico de un paciente a menudo se encuentra distribuido en distintos centros y nunca se llega a compartir con los demás, este aspecto conlleva a que en muchas ocasiones los pacientes y profesionales de la

sanidad tengan que repetir pruebas que ya habían realizado o incluso aplicar un tratamiento que el paciente ya pueda haber realizado en otro momento y no le haya surtido efecto, pero el profesional no lo sepa y se lo vuelva a recomendar.

Con la tecnología blockchain se plantea la posibilidad de superar estos problemas. La idea principal es la construcción de un sistema que permita a todos los profesionales compartir información entre los distintos centros médicos. Gracias a la aplicación de esta tecnología se podría conseguir:

- Control sobre el historial de cada uno de los pacientes, algo muy importante frente a posibles casos de negligencia, modificación de datos, conocer quien accede a los historiales de un paciente, etc.
- Información crítica y de cualquier ámbito de la salud de los pacientes constantemente actualizada sin que sea necesaria la realización de trámites externos para conseguirla.
- Control sobre las pruebas y diagnósticos dados al paciente, para así evitar duplicar pruebas que generan pérdidas de tiempo tanto al paciente como al personal de sanidad y además aumentan los costes.

Incluso en este aspecto, el historial médico de un paciente a través de blockchain podría incluir cualquier información relevante como resultados, tratamientos y enfermedades entre otras cosas que se le hubieran diagnosticado, incluso en hospitales privados porque se puede conseguir que todos los servicios sanitarios al alcance del paciente estén conectados con el objetivo de ofrecerle el mejor servicio posible. Se podría incluso gestionar la información procedente de dispositivos sanitarios tales como pulseras electrónicas, sensores de glucosa, marcapasos..., para así poseer toda la información clínica posible en tiempo real. (Laguna 2018)

Yendo mucho más lejos, podríamos imaginar incluso un ecosistema sanitario global y participativo. Se podría mantener con una plataforma adecuada basada en blockchain donde se tuvieran todos los datos y registros de salud unificados en lugar de tenerlos almacenados en distintas plataformas de diferentes formatos y sistemas. Con esta ambiciosa idea se podría tener todo tu historial médico en cualquier lugar del mundo a tu alcance, para que pase lo que pase y nos encontremos donde nos encontremos, el personal sanitario que nos atienda pueda contar con toda la información lo más actualizada posible sobre nosotros para realizar su trabajo con la mayor profesionalidad y seguridad posible.

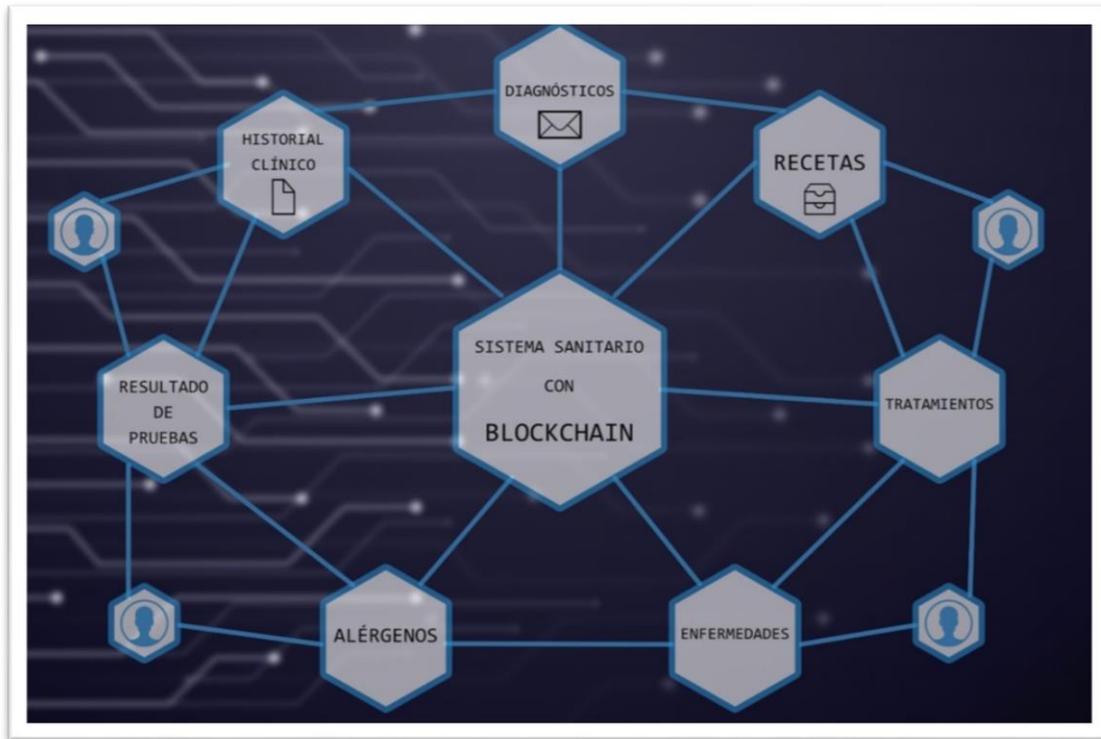
Según muchos expertos e inversores, tales como Jeremy Stone, “el sistema sanitario mundial está destinado a fracasar”. Estos expertos auguran que los actuales sistemas sanitarios son insostenibles debido al aumento de la población, la constante aparición de nuevas enfermedades, el aumento de la esperanza de vida, etc. Actualmente los sistemas sanitarios son en muchos casos ineficientes, sólo en EEUU se pierden anualmente una media de 150.000 millones de dólares por citas médicas perdidas.

Blockchain para muchos de estos especialistas es considerada una de las tecnologías que podría evitar el fracaso de los sistemas sanitarios, ya que podría analizar la salud de distinta forma a la actual, evitar procesos innecesarios, dar confianza, ser mucho más eficiente

en el tratamiento de datos y por lo tanto reducir los costes médicos y administrativos de todos estos procesos.

En la siguiente figura podemos observar un ejemplo de cómo blockchain podría conectar todas las ramas de la salud para una mejor comunicación y tratamiento de la información entre los distintos ámbitos del sector.

Figura 9.- Sanidad pública y privada con blockchain



Fuente: Elaboración propia

Son muchos ya los proyectos que existen o están en desarrollo por todo el mundo. A continuación vamos a nombrar alguno de ellos para conocer como se está enfocando la tecnología en la práctica:

- **Iryo:** se está creando a través de esta plataforma un registro único electrónico de sanidad en Eslovenia, para que sus pacientes puedan acceder a sus datos desde cualquier parte del mundo.
- **Chronicled:** se utiliza blockchain con esta aplicación para mejorar el mantenimiento y tratamiento de productos sensibles a las variaciones de temperatura y al paso del tiempo, tales como vacunas o medicamentos. Con este proyecto también se está intentando conseguir la detección de productos falsificados en las cadenas de suministro. Se trata de un proyecto utilizado en San Francisco (EEUU).
- **Medicalchain:** se basa en una plataforma blockchain que permite la creación de un registro electrónico inmutable que siempre y cuando lo permita el paciente, se puede compartir con médicos, hospitales, farmacéuticas y laboratorios entre

otros. Incluso permite el contacto entre pacientes y médicos a través de sesiones online. Se utiliza en Reino Unido y utiliza criptomonedas como pago por los servicios de salud.

- **Patientory:** nació en la ciudad de Atlanta (EEUU) y utiliza las cadenas de bloques para crear perfiles médicos de los pacientes donde se encuentren todos sus datos, sus visitas al médico, información sobre enfermedades y alérgenos, seguros médicos, etc.

Como hemos podido ver las opciones de blockchain en sanidad son múltiples y podrían facilitar muchos de los procesos actuales, pero todo depende de cuán dispuestas estén las organizaciones sanitarias y AAPP para crear y desarrollar las infraestructuras técnicas necesarias para su funcionamiento. Blockchain en este ámbito es nuevo y por lo tanto aún faltan muchos aspectos por pulir y alimentar lo que origina un proceso lento y costoso pero que sin duda puede aportar muchas ventajas para el futuro de la sanidad, tanto pública como privada. (Stone 2018)

Al igual que en el resto de aplicaciones de blockchain a la AAPP vistas hasta ahora, aún quedan muchos aspectos que mejorar, sobre todo temas relacionados con la ciberseguridad que sin duda es el aspecto más preocupante cuando hablamos de datos electrónicos. El potencial de blockchain es infinito siempre y cuando se consiga demostrar que se trata de una tecnología segura y que nuestros datos estarán seguros en la red frente a ataques de hackers.

Por lo tanto, la ciudadanía necesita confianza para comenzar a apostar en la tecnología y dejar que se administren sus datos médicos a través de ella. Cuando esto ocurra y cuando las AAPP apuesten al máximo por ella, quizás veamos un sistema sanitario utilizando blockchain para el tratamiento de información, consiguiendo reducir las listas de espera, los procesos, la burocracia administrativa y con todo ello disminuyendo el coste de la sanidad para las arcas públicas algo que nos beneficiaría a todos siempre y cuando la sanidad mantenga o aumente la calidad que ahora posee.

Mientras tanto, seguimos manteniendo el sistema sanitario actual, con cada vez más pinceladas de blockchain en él a través de distintas aplicaciones y plataformas como las antes comentadas que comienzan a facilitar los distintos trámites a realizar, con ellas podemos ver como blockchain se está haciendo un hueco y puede que de aquí a unos años esta pequeña introducción de la tecnología en el sector de la salud sea algo mayoritario y necesario para todos.

## 4. BLOCKCHAIN EN LA GESTIÓN DEL SISTEMA DEMOCRÁTICO

### 4.1 BLOCKCHAIN Y EL VOTO ELECTRÓNICO

El sistema electoral de un país es uno de los procedimientos más importantes de cualquier nación del planeta, especialmente cuando hablamos de estados democráticos. A través de estos procedimientos los países con democracia establecida seleccionan o eligen a los que serán sus líderes políticos para la siguiente legislatura o periodo de gobierno.

Estos sistemas se caracterizan por ser la forma de organización social que atribuye la titularidad del poder al conjunto de la ciudadanía. Los representantes de la ciudadanía son elegidos por estos mediante mecanismos de participación directa o indirecta que confieren legitimidad a sus representantes.

Históricamente la democracia se remonta a las antiguas civilizaciones que organizaron sus instituciones sobre la base de los sistemas igualitarios tribales o comunitarios. Posiblemente la primera democracia o por lo menos la más conocida es la de la antigua Grecia, donde en las polis apareció una asamblea del pueblo que fue el inicio de este sistema social a pesar de que en estas sólo podían participar los varones libres y por lo tanto el 75% de la población formado por mujeres, esclavos y extranjeros quedaba excluido.

En este apartado introduciremos de forma breve cómo funciona el sistema electoral español, para después analizar las posibles funcionalidades de blockchain en sistemas electorales y como podría mejorar a los actuales, a la vez que hablamos de los posibles riesgos o peligros que pudieran existir.

La aplicación de blockchain a los sistemas electorales es uno de los avances más importantes que pueden generar las cadenas de bloques en las AAPP.

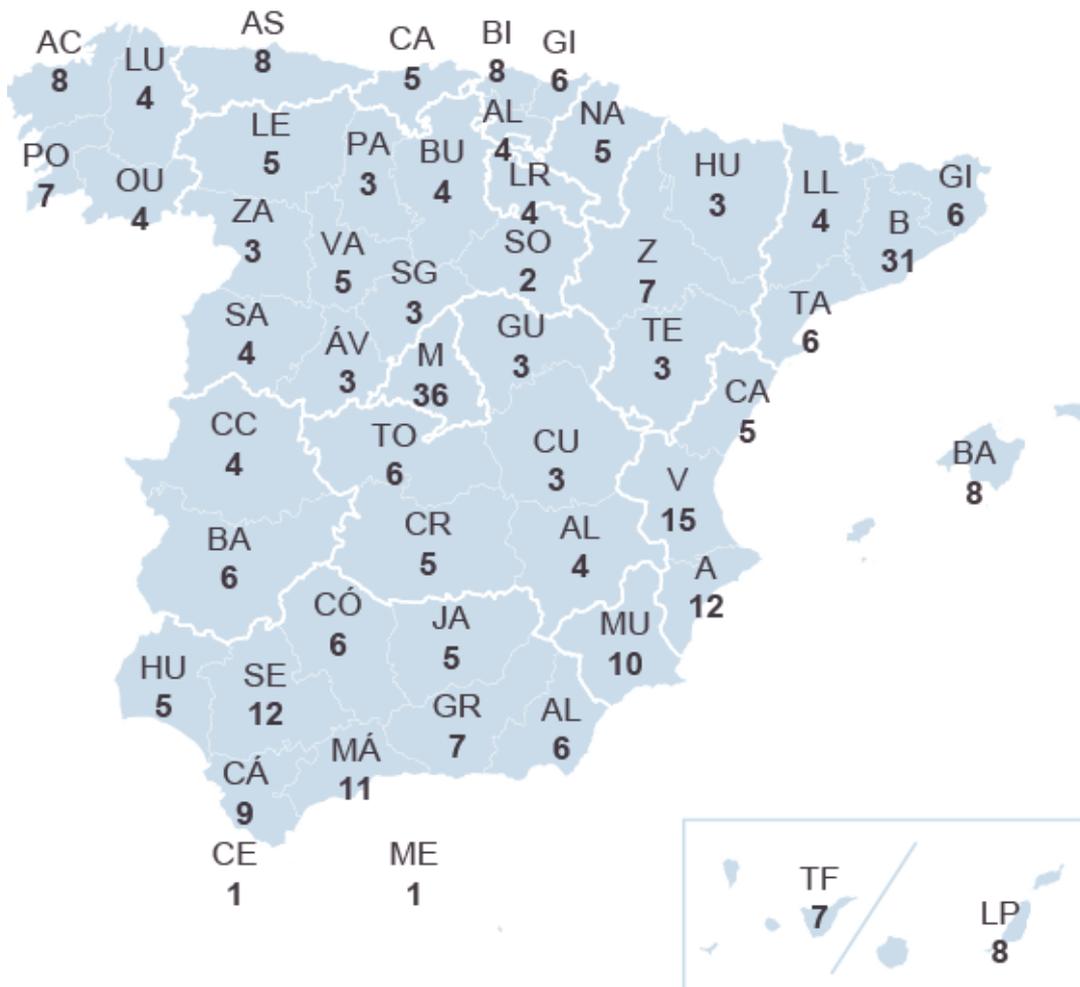
#### 4.1.1 SISTEMA ELECTORAL ESPAÑOL EN LA ACTUALIDAD

En este apartado vamos a hablar únicamente de las elecciones generales para hacernos una idea de cómo se realiza el proceso de votación por los distintos españoles y como se recuentan los votos, con el fin de ver posteriormente como ya hemos dicho que ventajas y desventajas puede tener un sistema electoral funcionando a través de blockchain.

En primer lugar tenemos que tener en cuenta que en las elecciones generales españolas se designan 350 diputados, los cuales están distribuidos en un total de 52 circunscripciones, que se corresponden con las 50 provincias más las dos ciudades autónomas (Ceuta y Melilla).

A cada provincia se le otorgan como mínimo 2 diputados y uno a cada ciudad autónoma, el resto un total de 248 diputados se asignan en función de la población de cada una de estas provincias, como es obvio las provincias con mayor población poseen un mayor número de diputados. El resultado del reparto es el siguiente:

Figura 10- Reparto de escaños de diputados por provincias



**Fuente: Ministerio del Interior**

Como ya hemos adelantado, son las provincias con una mayor población las que tendrán un mayor número de diputados. En las últimas elecciones fueron Madrid y Barcelona con 36 y 31 diputados respectivamente las provincias o circunscripciones con mayor número y tras estas podemos encontrar provincias como Valencia, Málaga, Sevilla y Alicante.

El número de diputados asignado a cada provincia no varía de forma significativa de unas elecciones a otras debido a que la población no cambia su lugar de residencia de forma continua y por lo tanto si se producen cambios son de pocos diputados y sobre todo como es normal estos cambios se sufren las provincias más rurales que pierden diputados por la despoblación hacia las zonas de costa o zonas más urbanitas donde la población sigue creciendo.

Para el reparto de estos escaños entre los distintos partidos políticos se utiliza la famosa Ley D'Hondt. Con este procedimiento se divide el número de votos emitidos para cada partido entre el número de cargos electos o diputados con los que cuenta cada circunscripción.

# Blockchain: Aplicaciones a la Administración Pública

Hay que tener en cuenta que sólo se consideran para esta ley los votos válidos y los votos en blancos, es decir, no se tienen en cuenta los votos nulos. También hay que considerar que se debe de tener un mínimo del 3% del total de los votos para poder aspirar a obtener representación. (Escudero 2015)

Por lo tanto y a modo de ejemplo, si consideramos que nos encontramos en la provincia de Ciudad Real cuyo número de diputados es en la actualidad de 5, vamos a imaginar que el partido A consiguió 5000 votos, el partido B un total de 4000 votos, el C 3500 votos y el partido D 1000 votos, para saber que partidos se quedan con esos escaños, dividimos los votos obtenido por cada una de las formaciones entre 1, 2, 3, 4 y entre 5 y cogemos los 5 resultados más grandes. El resultado final sería de 2 diputados para el partido A, otros dos diputados para el partido B y 1 diputado para el partido C, quedándose de esta manera el partido D sin representación en el congreso por esta provincia.

De manera visual quizás sea más fácil de comprender como se realiza el reparto entre las distintas formaciones políticas:

Figura 11- Reparto de escaños a través de la Ley D`Hondt

Partidos	Votos	÷1	÷2	÷3	÷4	÷5
<b>A</b>	5.000 Votos	5.000	2.500	1.666,6	1.250	1.000
<b>B</b>	4.000 Votos	4.000	2.000	1.333,3	1.000	800
<b>C</b>	3.500 Votos	3.500	1.750	1.166,6	875	700
<b>D</b>	1.000 Votos	1.000	500	333,3	250	200

Fuente: Elaboración propia

En cuanto a las características de la votación que más afectan a nuestro trabajo, hemos de decir que para poder votar en una determinada provincia hay que estar inscrito en el Censo Electoral de ese territorio. Antes de las elecciones la Oficina del Censo Electoral envía a cada uno de los votantes una tarjeta censal en la que se incluyen los datos personales de ese votante y se indica el colegio electoral donde tiene que ir a votar, es decir, el sitio físico al que debe ir el día de las elecciones.

El día de celebración de las elecciones cada votante se acerca a su respectivo colegio electoral y a su mesa de votación con los sobres de papel donde se encuentra su elección. Cuando se encuentra en su mesa de votación da su nombre y apellidos y el presidente y vocales de la mesa acreditan su identidad con ayuda del documento de identidad nacional u otro documento válido y es el momento en el que el votante puede ejercer su derecho a voto. Siempre hay excepciones como el voto por correo si no nos encontramos en nuestra ciudad el día de la votación, voto por correo que hay que solicitar con antelación si queremos que el día señalado podamos votar de esta forma, porque si no lo solicitamos perderemos el derecho a voto al no poder votar por correo por no haberlo pedido y tampoco de forma presencial porque como ya hemos dicho nos encontramos fuera de la ciudad.

Este voto por correo es utilizado normalmente por personas que se encuentran por motivos laborales o de ocio fuera de su ciudad, pero la mayoría de la población ejerce su derecho a voto de manera presencial.

Por otro lado, otra de las características principales del sistema electoral actual es la designación de presidentes y vocales para todas y cada una de las mesas electorales que se forman el día de las elecciones. Esas personas son seleccionadas de forma aleatoria y avisadas a través de correo de su obligación de personarse y realizar las funciones establecidas para ellos de manera obligatoria el día electoral. Sólo se puede evadir esa obligación en ciertos casos de fuerza mayor como pueden ser haber sido declarado discapacitado, estar en situación de incapacidad temporal para el trabajo con la correspondiente baja médica, en el caso de encontrarse en periodo de gestación a partir de los seis meses de embarazo y el periodo correspondiente de descanso maternal, lesión, dolencia o enfermedad física o psíquica y previsión de una operación quirúrgica entre otros casos.

De no encontrarse en ninguno de estos casos ni en los otros existentes, la responsabilidad de asistir a la jornada electoral como presidente o vocal será obligatoria.

El proceso de votación se puede explicar con mucha más profundidad debido a que existen multitud de variables y actores, pero para nuestro trabajo sólo necesitamos saber cómo funciona para entender mejor como puede ser el futuro con blockchain. Como hemos podido ver es un proceso bastante rudimentario para encontrarnos en el siglo XIX, más aún cuando ya podemos hacer cualquier tipo de gestión con conexión a Internet y desde nuestro hogar.

#### **4.1.2 ELECCIONES CON BLOCKCHAIN**

Con anterioridad durante los primeros epígrafes de este trabajo hemos podido comprobar que las características básicas asociadas a la cadena de bloques son inmutabilidad, participación libre, transparencia, seguridad, etc. Aspectos estos que nos pueden brindar una nueva perspectiva alrededor de los sistemas electorales.

Un sistema de votación basado en blockchain puede permitirnos que los votos sean seguidos, contados y correlacionados por muchas fuentes diferentes, lo que puede ayudar a mejorar la transparencia del sistema ya que todo puede ir comprobándose públicamente. Otra de las ventajas que a priori nos brindaría blockchain es la seguridad, gracias al uso de una criptografía potente. También se podría verificar el voto mucho más rápido que en la

actualidad, comprobando que se ha realizado correctamente y minimizando los errores humanos en el proceso de recuento en el que se requiere de gran cantidad de personas para poder realizarlo.

Otra de las ventajas a ofrecer por blockchain es la reducción del gasto público que supone celebrar unas elecciones generales o cualquier tipo de elección democrática debido al envío de propaganda electoral, las fuerzas del estado que velan por las seguridad durante la jornada electoral, las cantidades que se pagan a cada persona que es seleccionada a sorteo para estar en las mesas electorales como presidentes o vocales, la empresa que comunica el escrutinio, etc.

Podríamos también reducir el impacto ambiental que suponen unas elecciones sobre todo por el gasto en papel, ya que si imaginamos que en España hay 40 millones de personas en edad de votar, y se presentan a las elecciones 5 partidos, esto supone que hay que imprimir como mínimo 200 millones de papeletas, más un sobre para cada votante ya suman 240 millones de impresiones a papel, todo esto sin contar las papeletas de la cámara alta o senado y sus respectivos sobres. Pero por si esto fuera poco, cada partido envía a todos los hogares papeletas ya rellenas con su formación política, una para las cortes y otra para el senado, considerando que eran 5 partidos políticos con los que contábamos, serían 400 millones de papeletas más. Al final de todo, tenemos aproximadamente unos 720 millones de papeletas y sobres que podrían ahorrarse con un sistema electoral con base en blockchain.

Finalmente podríamos incluso pensar que los humanos pueden alterar la votación, como se ha demostrado en varias ocasiones y aunque hemos de decir que no es lo habitual, han existido casos en los que se ha alterado los resultados de alguna urna o alguna mesa electoral en favor de un partido político, aspecto que no podemos dejar obviar ya que siempre que algún proceso se realice por humanos de forma manual cabe la posibilidad de que exista algún tipo de fraude. (Maldonado 2019)

### **4.1.3 ESTONIA EL PAÍS DIGITAL POR ESCELENCIA**

Allá por el año 2000 Estonia declaró el acceso a Internet como un derecho humano básico, poniéndolo al mismo nivel que alimentos y hogares. Todo comenzó en 1991 cuando el país se independizó de la URSS, y decidieron comenzar su proceso de reestructuración como un país independiente apoyándose en la tecnología e intensificándose este proceso a raíz de sufrir uno de los ataques cibernéticos más importantes de la historia, que originó una interrupción temporal del país, el cual se estaba convirtiendo en el origen de muchos de los servicios digitales del momento. Todo esto le ha llevado a ser el país puntero en tecnología que ahora es.

En la actualidad, los servicios públicos del país están digitalizados y todos los ciudadanos tienen identidades digitales seguras que les permiten hacer cualquier trámite desde Internet, desde renovar el pasaporte hasta incluso crear una empresa y pedir recetas médicas, todo desde el sofá de casa sin moverse y con tan sólo un teléfono móvil en las manos.

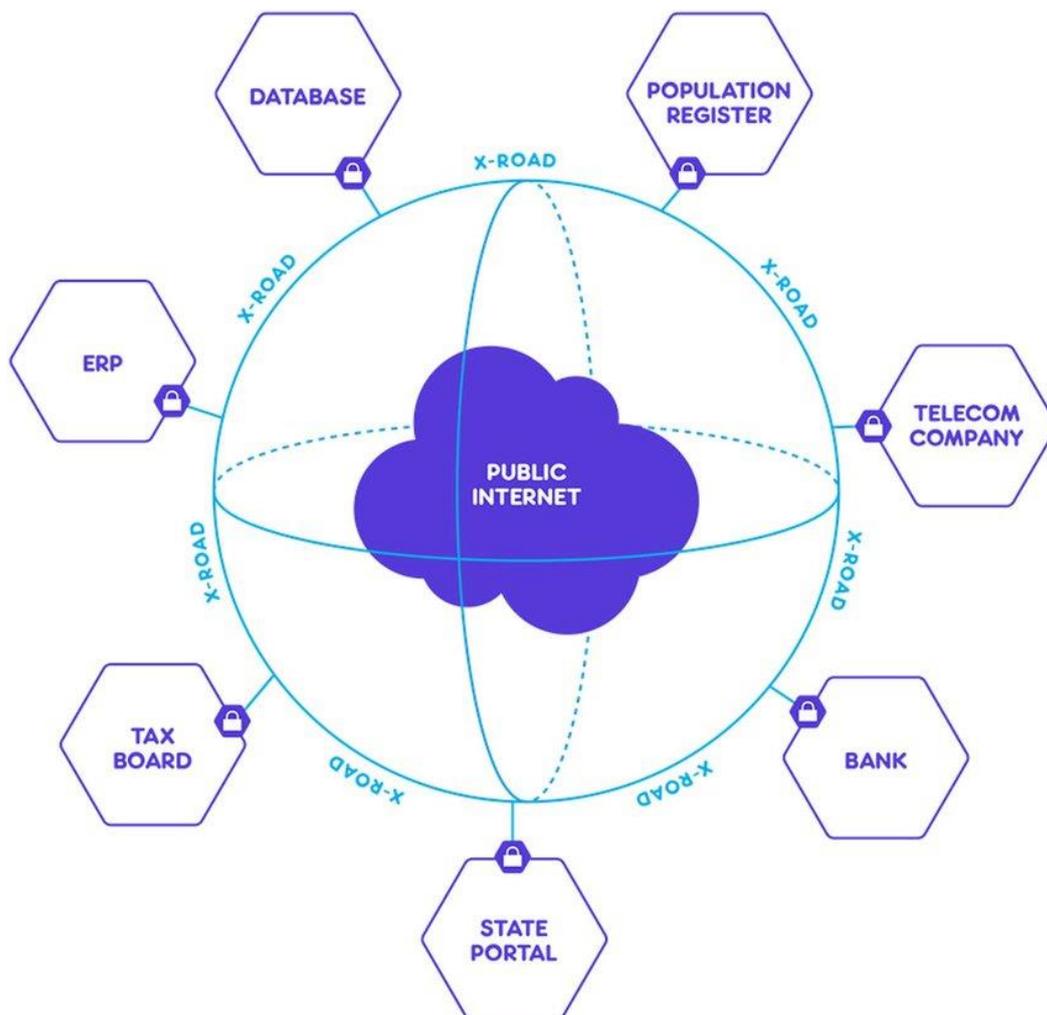
El protocolo que permite que los datos estén descentralizados y cifrados además de que nunca se dupliquen y se puedan compartir seguros por internet es el denominado “X-

**Road**". Este protocolo está asociado a blockchain, y permite que los datos de todos los ciudadanos sean confidenciales. Al ser un sistema que funciona con blockchain, no se almacenan todos los datos juntos, sino que se tienen las diferentes bases de datos separadas unas de otras, de forma distribuida.

En cuanto a su uso, los ciudadanos sólo se preocupan de llevar su DNI digital consigo y lo pueden utilizar para cualquier trámite, si por ejemplo mientras conducen les hacen un control los agentes de seguridad, con sólo enseñar el DNI digital pueden comprobar si tiene carnet de conducir en vigor, seguro en regla, etc. Además cada funcionario del estado sólo puede acceder a los datos que necesite estrictamente para desempeñar su trabajo, es decir, el guardia de tráfico del que hablábamos no podrá ver el expediente médico del conductor, aunque también se pueda acceder desde el mismo DNI, pero eso ya es competencia de su médico, al igual que el médico no puede saber si el paciente tiene multas de tráfico o no.

Para aumentar la seguridad ante posibles ataques, han decidido tener una copia de todos los datos fuera del país, es lo que conocen como "embajada de datos" y se encuentra en Luxemburgo.

Figura 12- La carretera X-Road



Fuente: Autoridad del Sistema de Información de Estonia

Si hablamos de lo que nos interesa en este epígrafe, es decir de elecciones democráticas con blockchain, debemos hablar de las elecciones en este país. A la hora de votar, los estonios tienen que registrarse previamente como votantes, contar con un dispositivo con conexión a internet ya sea un ordenador, teléfono móvil o tableta y con el DNI digital. El paso siguiente es descargarse la aplicación para votar y el software verificará automáticamente si la persona interesada en votar está capacitada para ello.

Una vez la persona en concreto ha decidido a quien votar y realiza el voto, la aplicación lo encripta y lo envía de manera segura a un servidor donde se recogerán todos los votos electrónicos, marcándose cada uno de ellos con una marca digital que posibilita poder revisarlos posteriormente si fuera necesario por cualquier tipo de problema.

Podemos pensar que como el voto electrónico no se emite desde un lugar de la AAPP y de manera presencial, una persona podría estar votando mientras es coaccionada por otra, por ello se permite volver a votar electrónicamente durante el periodo establecido que es el que comprende desde el décimo hasta el cuarto día previo a las elecciones presenciales, o incluso, si esto no fuera posible puede acudir finalmente de manera presencial a votar el día de las elecciones. Obviamente si una persona vota dos veces sólo se tiene en cuenta uno de los votos, que en estos casos sería el último que haya realizado.

Las últimas elecciones generales que se celebraron en el país el 3 de Marzo, el voto online con blockchain tuvo un gran éxito ya que casi la mitad de los votantes totales lo hizo a través de Internet, en concreto un 44% de los votantes, cifra que ya es bastante importante y que aumenta elección tras elección.

A parte de utilizar blockchain para votaciones generales de un país, existen muchos casos en los que se ha aplicado para el sector privado, algunos de ellos son:

- **Abu Dhabi Securities Exchange (ADX):** se trata del mercado de valores de Abu Dhabi, el cuál a finales del año 2016 comenzó a trabajar con blockchain para establecer un sistema de votación que permitiese a los accionistas de las empresas que cotizaran en el mercado poder conectarse en directo y de forma remota desde cualquier lugar para participar en las votaciones y monitorizar los resultados a distancia durante las juntas generales anuales.
- **SettleMint:** se trata de una startup belga que fue adquirida por Overstock, empresa que comercializa productos por Internet, ha creado una plataforma blockchain para empresas que les permite realizar procesos de votación internos, agilizar y facilitar diversos trámites dentro las propias empresas como el registro de clientes y proveedores, la autenticación de información, facilidades en el proceso de auditoría, etc. Además Overstock se ha convertido en la primera gran empresa en pagar sus impuestos con Bitcoin, aspecto nos hace pensar lo introducida que está la compañía en las tecnologías.
- Son muchos los partidos políticos que han utilizado tecnología blockchain para realizar elecciones internas, como el Partido político Liberal Alliance y el partido político Unidas Podemos este último de España.

Figura 13.- Voto electrónico con blockchain



Fuente: criptonoticias.com

#### 4.1.4 ¿POR QUÉ EL VOTO ELECTRÓNICO NO ES UNA REALIDAD EN NUESTRO PAÍS?

Como hemos podido ver parece que las ventajas de un sistema electoral basado en blockchain son innumerables y agilizarían en gran medida el proceso, facilitando especialmente a los ciudadanos residentes fuera de España que ejercieran su derecho a voto en nuestro país sin ningún tipo de problema a través de Internet.

Pero ¿por qué si son tantas las ventajas, el sistema electoral con blockchain todavía no es una realidad?

En primer lugar, debemos considerar la falta de confianza y de cultura digital del ciudadano español, cambiar del sistema “de toda la vida” en papel a uno totalmente por Internet crea dudas en la población que necesita un cambio de mentalidad apoyado desde las instituciones y sus líderes para acabar creyendo que este tipo de tecnologías facilitarían el proceso. Pero este cambio no se consigue de un día para otro, se necesita un cambio en la cultura, en la mentalidad de los españoles. Quizás haga falta mayor información sobre los principales aspectos de esta tecnología para que la confianza en ella crezca, porque de no tener la confianza de toda la población, el sistema no tendría total legitimidad.

Se tiene que conseguir que utilizar la tecnología blockchain sea tan común como ir a trabajar, al supermercado o cualquier trámite de la vida cotidiana de los ciudadanos, aspectos que se han conseguido en otros países como Estonia y que crean esperanza para los defensores de la tecnología.

Otro de los factores a tener en cuenta no es otro que el miedo a sufrir ataques de hackers, que por muy seguro que sea el sistema, siempre existirá cuando hablemos de Internet. Son muchos los expertos en ciberseguridad que se oponen a las votaciones online de cualquier tipo porque consideran que es insegura. Estos expertos explican que una cadena de

bloques no puede proteger la información mientras viaja a través de internet ni garantizar que el voto de los usuarios se registre correctamente, mientras en el sistema tradicional, los votos están distribuidos en mesas electorales por todo el país, todas estas son independientes unas de otras y por ello si se manipula una mesa, sólo afectará a los votos de esa sin alterar los del resto de los ciudadanos, llevar esta característica a un sistema electrónico es mucho más complicado de lo que parece.

La tecnología además de ser segura y común para la ciudadanía, debe de ser fácil de usar. Es imprescindible que los ciudadanos se sientan cómodos con blockchain para poder tener una buena impresión de la cadena de bloques. Pero para esto falta una mayor concienciación y educación en materia tecnológica de las personas, en nuestro país todavía hay un grueso importante de la población sin conocimientos informáticos, aspecto que dificulta la implantación de sistemas totalmente tecnológicos.

#### 4.1.5 CONCLUSIONES

A lo largo de este epígrafe hemos podido conocer cómo funciona de manera general el sistema electoral español, un sistema democrático en el que los ciudadanos al igual que en la mayoría de países del mundo deben ir a votar de forma presencial y a través de votos impresos en papel.

Actualmente son muchas las alternativas que están surgiendo a este tipo de sistema, y una de las más nombradas y que como hemos podido ver ya se utiliza en países como Estonia es el voto electrónico u online con blockchain.

Hemos podido ver las ventajas que este tipo de sistemas pueden aportar frente a los sistemas actuales pero también que se corren riesgos que en la actualidad no existen. Está claro que en un futuro cercano se comenzará a probar este tipo de sistemas como alternativa a los tradicionales porque la sociedad evoluciona y sus formas de vida cambian hacia unas más tecnológicas y conectadas a Internet. Por ello pienso que blockchain sí que puede tener cabida en las elecciones nacionales de la mayoría de países, pero siempre y cuando se solucione o mejore los posibles riesgos que estas elecciones puedan suponer. Ya tenemos un ejemplo de aplicación de esta tecnología en un país democrático de la Unión Europea como es Estonia y es seguro que el resto de países se están fijando en él como posible ejemplo para una futura aplicación de la tecnología.

Actualmente en nuestro país la población no se encuentra preparada al cien por cien para celebrar unas elecciones con blockchain sólo, porque como ya hemos comentado muchos ciudadanos no tienen acceso a Internet o no poseen los conocimientos necesarios para ejercer su derecho a voto vía online. Esta situación no evita que un gran número de ciudadanos sí que estén dispuestos a probar nuevas alternativas que le faciliten la forma de votar, que permitan reducir gastos al Estado, que eviten a muchas personas tener que ir de forma obligada el día de las elecciones a “trabajar” como presidente o vocal de una mesa cuando normalmente al celebrarse las mismas un domingo, es día festivo o de descanso para la mayoría de ellos y no deberían de estar allí de forma obligada aunque les paguen, que consigan eliminar la intromisión de personas en el recuento de votos porque aunque sea difícil siempre se pueden llegar a alterar los resultados, etc.

Todo esto si nos fijamos en las características de nuestro país, pero si pensamos en países donde la democracia no está tan extendida o nos encontramos con una democracia ficticia y se sabe que las elecciones son amañadas por políticos, grupos de empresas, grandes inversores..., la tecnología de la cadena de bloques puede ayudar en gran medida a la reducción de este tipo de comportamientos inmorales e incívicos que en cualquier lugar del mundo la población rechaza y no acepta. En estos países, normalmente subdesarrollados o en vías de desarrollo, blockchain puede ofrecer grandes oportunidades para el desarrollo de sus políticas y sistemas electorales, siempre teniendo en cuenta que otro de los problemas de muchas de estas regiones es la falta de acceso a Internet algo imprescindible para el uso de esta tecnología y que sin esta conexión difícilmente podrán desarrollar estas opciones de la cadena de bloques. No obstante, son posibilidades lejanas para estos países pero que algún día puede que barajen.

Por lo tanto, cuando se consiga reducir el riesgo de sufrir ataques cibernéticos al mínimo, cuando la población sea consciente de las ventajas de esta tecnología y cuando los políticos estén dispuestos a introducirla, estoy seguro de que podrá encajar como alternativa al sistema electoral actual de nuestro país.

Siempre con una introducción progresiva y sin llegar a eliminar el sistema tradicional para que los ciudadanos puedan decidir que opción de votación prefieren ya sea por voto electrónico o por el sistema tradicional. Con esto se conseguiría dar más opciones a los habitantes de un país para que se sientan más cómodos ejerciendo su derecho a voto y que todos los ciudadanos que ahora mismo les es complicado ejercer este derecho por su situación personal o laboral, tengan una alternativa fácil y segura para poder participar en el sistema democrático de su país.

## 4.2 CATALUÑA Y BLOCKCHAIN

Si en España tenemos que destacar una comunidad autónoma en la cual se esté apostando por la tecnología de la cadena de bloques, esa es sin lugar a dudas Cataluña. Tras utilizar la tecnología blockchain, en concreto la plataforma Ethereum de la que ya hemos hablado con anterioridad, para la realización del referéndum del 1 de octubre de 2018 durante el mandato de Carles Puigdemont, ahora el Gobierno de Cataluña ha aprobado la primera Estrategia Blockchain de Cataluña con la que pretende introducir esta tecnología en las AAPP de la comunidad.

A lo largo de la estrategia aprobada, se desarrollan cada uno de los ámbitos sobre los que se va a trabajar e introducir la cadena de bloques. Estas áreas van a ser seis e incluyen administración, promoción, innovación, ecosistema de emprendimiento, talento y marco regulatorio. Con esto, el Govern espera situar a Cataluña como un referente en el uso y el desarrollo de las tecnologías de registro distribuido como es blockchain a la vez que se aumenta la transparencia y se consigue garantizar la confianza ciudadana.

Como dijo Jordi Puigneró, actual consejero de políticas digitales y administración pública de la Generalitat, "blockchain tiene potencial para general la misma revolución que generó Internet en su día"

Los objetivos en las seis áreas de actuación comentadas son los siguientes:

**Administración:** se pretende mejorar los servicios públicos para la ciudadanía, favoreciendo una prestación de servicios proactiva, es decir, adaptada a los cambios y en constante actualización, y personalizada. Se pondrá en funcionamiento un entorno de pruebas y el Observatorio de Tecnologías Blockchain y DLT (tecnologías de registro distribuido).

**Promoción:** se quiere mostrar a Cataluña como referente en la utilización de la cadena de bloques y el resto de tecnologías distribuidas. Dos de los eventos destacados en este aspecto son “Blockchain Solutions World” y “Barcelona Blockchain Week”.

**Ecosistema de emprendimiento:** se pretende potenciar una nueva industria, mucho más tecnológica y dinamizar la demanda de servicios y soluciones a través de programas de emprendimiento. También crear espacios de emprendimiento para las empresas de los distintos sectores y un programa de dinamización de soluciones verticales adaptadas a las necesidades de los diferentes sectores.

**Innovación:** en este aspecto se pretende crecer a través de centros de investigación, tecnológicos y el desarrollo de entornos para la innovación como “Catalonia Blockchain Living Lab”, así como el impulso de proyectos de I+D+I que consigan enlazar la tecnología blockchain con la inteligencia artificial y las redes 5G.

**Talento:** se quiere situar a Cataluña como el lugar idóneo para formarse y desarrollar tu carrera profesional, por ello el objetivo es generar, retener y atraer talento. La iniciativa se fomentará entre otros con el nombre de “Barcelona Digital Talent”.

**Regulación:** creación de un grupo de trabajo que se encargue de analizar la normativa y definir un margo regulatoria favorable para el desarrollo de blockchain y en especial tratando el tema de la protección de datos tan importante cuando se pretende tener la información de la población en internet.

Esta estrategia es el resultado de más de un año de trabajo tras la decisión del gobierno de la Generalitat de Cataluña de implementar la tecnología en la AAPP. Para conseguir este fin se creó un grupo de trabajo que consiguiera impulsar esta tecnología y las conclusiones a las que han llegado estos expertos son las bases sobre las que se ha elaborado el documento o la estrategia que ahora han aprobado. (Merchan 2019)

Estos son algunos de los proyectos que están en marcha o que comenzarán a funcionar próximamente:

- Mejora de la gestión de los residuos.
- Sistema de identificación verificada de Cataluña.
- Registro de consentimiento.
- Apoyo a la transición energética hacia las energías renovables, a la vez que se impulsa y permite el autoconsumo fotovoltaico del ciudadano que sea capaz de generar su propia energía y almacenarla. Después los ciudadanos que hayan generado y almacenado esta energía, podrán “venderla” a cambio de recompensas en forma de criptomonedas que aún están por ver.

- Canal seguro entre el Parlamento y la Generalitat de Catalunya, que consistirá en un sitio web para el envío y almacenamiento seguro de mensajes y datos.
- Apoyo en el trasplante de órgano, esto se puede conseguir con blockchain a través de una red que permite compartir datos e indicadores biológicos entre los distintos hospitales para conseguir una selección mucho más eficiente y precisa de los posibles receptores en casos de trasplantes de órganos.

## 4.2.1 PROYECTO “IoCat”

Como hace un momento adelantábamos, uno de los proyectos en los que la Generalitat de Cataluña contempla utilizar blockchain es para el apoyo a la transición energética, proyecto este denominado como “IoCat”.

Fue la consejera de Empresa y Conocimiento, Ángeles Chacón, la encargada de dar a conocer a los medios este proyecto a través del cual y con la ayuda de los ayuntamientos catalanes se espera que los ciudadanos de la región puedan hacer transacciones de la energía que ellos mismos hayan generado y almacenado. Estas transacciones se podrán realizar de manera fácil, segura y ahorrando en costes y tiempo de intermediarios gracias a la utilización de blockchain. Los ciudadanos que “vendan” esta energía podrán obtener recompensas en forma de criptomoneda que todavía está por crear pero con la cual se pretende impulsar el autoconsumo fotovoltaico.

Esto ayudaría a cumplir con las exigencias de Europa a las que el Govern se comprometió y en las cuales se espera que para 2030 el 32% de la energía consumida por la comunidad provenga de fuentes de energía renovables.

Este proyecto se implementará a través de la red de Ethereum, que estará enlazada con redes independientes de energía solar que serán manejadas por los vecinos de las distintas zonas y las cuales funcionarán aisladas de las redes comerciales que todos usamos, para así poder captar su propia energía mediante placas solares.

Como cabe la posibilidad de que por ejemplo una comunidad de vecinos genere más energía de la que pueda consumir, se está barajando la opción de que estos productores independientes puedan vender los excedentes a otros vecinos utilizando una criptomoneda que como ya hemos comentado debería crearse para que pueda servir como moneda de cambio y se pueda producir el intercambio de energía entre vecinos.

## 4.3 TIVI

Como ya comentábamos al comienzo de este capítulo cuando hablábamos de blockchain y el voto electrónico, en la actualidad se están experimentando multitud de cambios en cuanto a la forma de desarrollar los sistemas de votación.

Hoy en día las AAPP se enfrentan a una ciudadanía moderna que viaja, que se muda a buscar nuevas oportunidades en el extranjero, ciudadanos demasiado ocupados por motivos laborales y ocio, ciudadanos con discapacidad que les dificulta votar en una mesa electoral, o simplemente que reclaman servicios más accesibles a la hora de ejercer su derecho a voto. Por

todo esto los sistemas de votación electoral actuales se están quedando cortos para muchos de estos ciudadanos.

Una de las opciones que han surgido tras esta situación es “TIVI”, solución de votación en línea conveniente y segura que permite a los gobiernos conectarse con sus votantes remotos al proporcionarles una plataforma transparente y universalmente verificable.

Este tipo de votación remota presenta una serie de ventajas a explotar frente a los sistemas tradicionales. TIVI asegura la privacidad del voto al igual que en el sistema actual, reduce la coacción de los votantes y elimina el fraude electoral y la manipulación de los votos por personas físicas.

Esta aplicación se ha basado para su desarrollo en el protocolo de votación utilizado en Estonia en sus últimas elecciones y que como ya vimos ha ido creciendo en popularidad entre los votantes año tras año. Y es que TIVI es el resultado de la formación en 2014 de un centro multidisciplinario de investigación y desarrollo que tenía como objetivo avanzar en la votación en línea. En este proyecto participaron Smartmatic y Cybernetica.

Smartmatic es una empresa privada fundada en los Estados Unidos en el año 2000 y que se ha convertido en el mayor proveedor mundial de tecnologías y soluciones de votación. Actualmente de entre los ochos países que se han lanzado como pioneros en la automatización de elecciones, esta empresa proporciona servicios y tecnología a seis de ellos: Filipinas, Estados Unidos, Venezuela, Estonia, Brasil y Bélgica.

Cybernetica por su parte es una empresa privada con sede en Tallin, Estonia. Compañía de ciberseguridad que se ha ganado una importante reputación como proveedor de soluciones innovadoras de gobierno electrónico y que formó parte del Instituto de Cibernética de la Academia de Ciencias de Estonia. Uno de sus proyectos más conocidos y por el que adquirió buena fama es el ya nombrado “X-road” de Estonia, además de desarrollar el primer sistema seguro de votación por Internet del mundo en este mismo país, que se ha convertido en el sistema de votación en línea más exitoso del planeta.

Esta aplicación ya se ha utilizado en distintas votaciones en diferentes partes del mundo, entre las que podemos destacar cuando fue utilizada por el Partido Republicano de Utah en marzo de 2016 para que los miembros de este partido pudieran emitir su voto. Estas elecciones se convirtieron en una de las experiencias de votación en línea más grandes en la historia de las elecciones estadounidenses.

En este caso, casi el 90% de los votantes que estaban registrados para votar en línea lo hicieron y con ello se consiguió una de las tasas más altas de votación, con votantes en línea que iban desde las personas más jóvenes hasta personas con 80 años ejerciendo su derecho a voto con TIVI. Además TIVI consiguió que los republicanos de Utah pudieran votar desde más de 45 países, consiguiendo de este modo unas elecciones con un alto grado de participación, ya que se recibieron votos de países como Japón, Sudáfrica y la Polinesia Francesa. (TIVI s.f.)

Con este tipo de aplicaciones desde mi opinión no debemos buscar eliminar los sistemas de votación tradicionales, pero sí se puede buscar una coordinación completa entre ambos, para poder facilitar al máximo las jornadas electorales a los participantes. Pensamos

que se pueden complementar con el fin de dar el mayor número de soluciones posibles a los ciudadanos que les permitan ejercer un derecho básico como es el del voto democrático con las mayores facilidades y garantías posibles. Si en la actualidad disponemos de la tecnología y conocimientos suficientes para desarrollar y aprovecharnos de estas nuevas opciones ¿Por qué no hacerlo? ¿Por qué no explotarlas para nuestro beneficio?

Aún queda mucho por desarrollar pero poco a poco se irán introduciendo estas tecnologías como alternativas a los métodos tradicionales, porque la sociedad evoluciona y con ella sus formas de vida y ahora en un mundo en el que prácticamente todo lo tenemos disponible en Internet, seguir desarrollando el voto a través de una mesa electoral y de forma presencial como única opción para la mayoría de los ciudadanos quizás se quede un poco obsoleto.

## 5. CONCLUSIONES

Finalmente, tras haber desarrollado todo el proyecto de final de grado, nos proponemos a desarrollar una serie de conclusiones relacionadas principalmente con los objetivos preestablecidos al comienzo del trabajo y con las distintas aplicaciones de blockchain para las AAPP que hemos podido desarrollar durante el mismo.

A lo largo de este trabajo pretendíamos entender y conocer con mayor profundidad las características básicas de blockchain que nos permitieran hacernos una idea de cuál es su potencial para muchos ámbitos de nuestra vida, principalmente los relacionados con las AAPP y su entorno.

A pesar de que el uso de esta tecnología está mucho más extendido en sectores como las finanzas y que la recopilación de una cantidad importante de información relacionada con blockchain en las AAPP puede resultar difícil porque todavía no se ha extendido su uso o muchas de las iniciativas que están en funcionamiento son simples proyectos que están en fase de prueba de viabilidad..., hemos podido encontrar y exponer distintas opciones donde la cadena de bloques se podría o incluso se está utilizando ya para mejorar los procesos públicos.

Una vez hemos analizado la tecnología parece quedarnos claro que la cadena de bloques gracias a sus características puede ofrecer multitud de oportunidades a la mayoría de procesos que día tras día realizamos los humanos. Hemos podido ver como mejoraría la logística de muchas empresas de transportes, los servicios tales como los conocemos con intermediarios podrían cambiar pasando a necesitarse cadenas mucho menos extensas de personas o empresas consiguiendo el mismo resultado y ayudándonos a ahorrar en tiempo y costes, e incluso hacernos la vida diaria mucho más fácil con las ciudades y casas conectadas, donde como vimos podemos llegar a esperar que en un futuro sea la nevera la encargada de avisarnos que alimentos necesitamos comprar o el coche avisarnos que necesita que cambiemos las ruedas porque ya están desgastadas entre otras muchas funciones.

Pero si nos centramos en los usos que hemos podido desarrollar para las AAPP, podemos ver como muchas de las administraciones que son clave para el funcionamiento de los Estados tal y como los conocemos actualmente se verían beneficiados por la cadena de bloques, ya que esta es capaz de aportar ventajas a todas ellas, y podemos destacar las tres siguientes:

- En el caso de la justicia, blockchain con aplicaciones como Kleros sería capaz de ahorrar en procesos e intermediarios, facilitando la tramitación de los procesos judiciales. Se permitiría reducir el tiempo de espera en la celebración de juicios, ya que muchos de los problemas que existen en la actualidad y que no son de verdadera importancia como una simple disputa entre dos personas por una mínima cantidad de dinero, podría resolverse e incluso evitarse si se realizara un Smart contracts. Hemos visto como es la propia plataforma la que determina quien lleva la razón en función del acuerdo o contrato y de los resultados de lo establecido.
- Otro de los aspectos básicos de cualquier Estado es su sistema sanitario. Gracias a la introducción de blockchain en un sistema sanitario moderno se

permite la conectividad de todos los datos de los pacientes para que en cualquier momento y en cualquier lugar, cualquier profesional de la sanidad disponga de toda la información relativa al paciente. Con esto logramos evitar que se repitan pruebas y tratamientos y de este modo ahorrar dinero y reducir las listas de espera que tanto empeoran el servicio sanitario de nuestro país por ejemplo.

- Otra de las mejoras que puede aportar la cadena de bloques a nuestras AAPP es en la gestión del sistema democrático, aunque todavía no se ha postulado como una opción por nuestros dirigentes, blockchain ha demostrado en otros países como Estonia y además nosotros lo hemos visto que puede ser un complemento perfecto en la forma de desarrollar las elecciones democráticas de un país. A pesar de que este cambio todavía no ha llegado a nuestro país, blockchain sí que ha sido utilizado por partidos políticos como Unidas Podemos para la celebración de elecciones internas.

Con la ayuda de la cadena de bloques se pueden celebrar elecciones democráticas con un menor impacto ambiental, con un coste para los contribuyentes menor, con un escrutinio fiable y al momento, facilitando a los votantes que voten desde casa, etc.

Blockchain ofrece un modelo de transparencia abierto y participativo para todos estos servicios y que a la vez los datos de los millones de ciudadanos del mundo se encuentren seguros y sin posibilidad de ser violados por ataques cibernéticos.

Como hemos comentado a lo largo del proyecto, una de las preocupaciones de nuestra sociedad es la falta de creencia en muchas de las instituciones públicas de las que dependemos. Esta situación deriva de los numerosos casos de corrupción y fraude que la población ha sufrido de parte de sus dirigentes. Esta visión negativa hacia la AAPP que muchos de los ciudadanos comporten puede ser modificada gracias a blockchain ya que al tratarse de una tecnología descentralizada y distribuida permite que sean los nodos participantes en el proceso los que se encarguen de que todo ocurra de forma correcta a través de los distintos procesos de consenso que hemos podido estudiar. Con esto evitamos que una autoridad central o una institución (pública en este caso) ostente todo el control sobre el proceso al tratarse de sistemas centralizados.

Por otro lado, plataformas como BenBen que pueden parecer a priori usos de blockchain para situaciones privadas más que para las AAPP, pueden ser usadas también por las AAPP de muchos países para situaciones similares para las que son usadas en la actualidad. Estamos seguros que este tipo de aplicaciones tendrán éxito y su uso se extenderá por multitud de países con similitudes a Ghana.

Para culminar este proyecto, podemos decir que hemos alcanzado los objetivos que desde un principio nos marcamos y que la tecnología de la cadena de bloques ha sido comprendida y extrapolada a posibles usos en las AAPP. Al comienzo del TFG nos proponíamos varios objetivos secundarios que nos llevarían a conseguir el objetivo principal.

Estos objetivos de segundo grado han sido alcanzados al entender a la perfección cuales son los rasgos básicos de la cadena de bloques y cómo es su funcionamiento. También

hemos estudiado que puede haber cadenas públicas y privadas, abiertas y cerradas y cuáles son las diferencias entre ellas. Hemos visto como blockchain ya está siendo utilizada y fomentada por el sector privado, principalmente por sectores como las finanzas y la energía. Viendo como las grandes compañías del planeta están apostando por ella y se están desarrollando consorcios de empresas para el desarrollo de soluciones con blockchain. Como las patentes con intrusión de cadenas de bloques no paran de crecer y cómo las grandes potencias mundiales como EEUU y China se esmeran por fomentarla en sus servicios.

Con todo esto hemos podido mejorar nuestra visión sobre esta tecnología y comprender como su potencial puede beneficiar a las AAPP. Hemos comentado con anterioridad en este capítulo de conclusiones como puede ayudar la cadena de bloques a muchos de los procesos que desarrollan las instituciones públicas y por lo tanto alcanzado el objetivo principal del proyecto que no era otro que entender el funcionamiento y potencial de blockchain para poder ver que usos puede desempeñar dentro de las AAPP.

En los capítulos tres y cuatro hemos visto varios usos de la cadena de bloques en las AAPP comprobando que puede mejorar muchos de los procesos, sobre todo los referidos a tiempos de espera y ahorro de costes a la vez que permite que estén descentralizados lo que puede ayudar a que la reputación de políticos y administraciones mejore al no tener estos poderes omnipotentes sobre todo el proceso.

Su potencial puede utilizarse en muchos otros casos que quizás todavía no se hayan explotado pero que seguro se explotarán en un futuro cercano. Blockchain tiene mucho que aportar a nuestras vidas, sin embargo muchos de los mejores expertos en ciberseguridad siguen sin terminar de confiar en la tecnología y eso da que pensar. Una de las características principales es la seguridad y estos expertos la ponen en duda, debido a que se ha demostrado que puede sufrir ataques al igual que todos los servicios que estén conectados a la red.

Estos expertos consideran que romper la seguridad de estas blockchain supone un coste muy elevado como ya dijimos durante el TFG pero que a su vez es matemáticamente posible y si existe la posibilidad puede que ocurra alguna vez. Además también consideran que con la llegada en un futuro de la computación cuántica el proceso de sabotear una red blockchain será más fácil.

Estos problemas de seguridad se terminarán limando quizás usando algoritmos post cuánticos y haciendo que la tecnología tenga mucho que ofrecer y poco en lo que temer. Con el paso del tiempo los aspectos negativos de esta como la comentada seguridad se rectificarán y la cadena de bloques se convertirá en parte de nuestras vidas facilitándonos multitud de procesos y operaciones que realizamos diariamente, desde saber que productos necesita nuestra nevera hasta ofrecernos tramitar la venta de nuestro hogar sin necesidad de intermediarios que ofrezcan confianza al proceso pero que aumenten los costes de esa venta, porque el proceso se podrá realizar con blockchain.

Pero antes de que esto ocurra se necesitan dos cosas muy importantes, la primera de ellas y como ya hemos dicho en multitud de ocasiones a lo largo de los distintos epígrafes, la sociedad necesita un cambio de mentalidad para poder confiar en una tecnología que actualmente la mayoría de ellos desconoce. Este proceso será lento e irá ocurriendo con el

paso de los años al igual que otros muchos hábitos se han introducido en nuestras vidas sin apenas ser conscientes de ellos.

Todavía nos encontramos en una sociedad anclada a aspectos antiguos a pesar de disponer de la tecnología suficiente para cambiarlos. Por ejemplo, recuerdo las clases de Banca y Bolsa donde el profesor durante las prácticas de laboratorio nos preguntaba quién de nosotros usaba dinero físico y quien tarjeta, quién usaba aplicaciones como Bizum cuando se juntaba con amigos para hacer un regalo o una fiesta, quien pagaba sus gastos como el gimnasio con efectivo o mediante transferencia...

Pues a pesar de estar en el siglo XXI y de poseer en la mayoría de comercios en los que compramos datafonos, de tener la posibilidad de pagar con el móvil... la mayoría de nosotros respondíamos que preferíamos llevar dinero en efectivo o que aplicaciones como Bizum para pagar al instante a un amigo todavía no las habíamos usado.

Esto habla de que todavía queda mucho por cambiar en nuestra mentalidad, que el cambio tecnológico está ocurriendo y es una realidad pero que mucha población sigue apostando por los medios tradicionales para muchas de sus operaciones y al igual ocurrirá con blockchain por ello es necesario tiempo y paciencia para que su introducción en la sociedad se haga efectiva.

Por lo tanto, quizás dentro de unos años tengamos una AAPP mucho más tecnológica, donde los ciudadanos tengamos identidades digitales que nos permitan realizar cualquier trámite de una manera mucho más eficiente y sin tener la duda de que nuestros datos pueden ser robados.

El segundo aspecto importante a impulsar es la creación de un marco normativo único que regule la tecnología, porque esto ofrecerá mayor confianza en ella y que los distintos países apuesten por ella de forma más rotunda, y para que esto ocurra la Unión Europea ya anunció la creación de un Observatorio de blockchain que estudie la tecnología y su aplicación a las AAPP.

Desde un punto de vista más personal, entiendo la tecnología de la cadena de bloques como una gran oportunidad para mejorar en el ahorro de tiempo y dinero, para ofrecer una mayor participación ciudadana en todos los procesos públicos, para evitar que un único organismo en el caso del sector público o una única empresa en el sector privado controlen todo el proceso, para permitir a las personas ser partícipes de estos procesos, etc.

A su vez considero por mi cierta aversión a que todo esté digitalizado que a pesar de que la seguridad se presenta como uno de los rasgos principales de blockchain, si los expertos en seguridad admiten que todavía queda mucho por hacer para conseguir que sea cien por cien segura es porque existen riesgos en su uso.

Por esto pienso que la cadena de bloques va a ser una parte importante en nuestras vidas en un futuro cercano pero que todavía no está preparada para introducirse en todos los procesos públicos que conocemos. Los datos de los millones de personas que vivimos en un país poseen un valor incalculable y existen multitud de usos deshonestos de ellos, por ejemplo, si imaginamos tener una sanidad pública conectada a blockchain, si la red sufriera un ataque

cibernético capaz de burlarla, los datos de todos los pacientes estarían en manos de personas que no deberían conocer esa información.

Sin embargo a pesar de esta cierta aversión a que todo esté digitalizado y a un clic de nosotros, debemos admitir que blockchain se postula como una tecnología revolucionaria, que ya está cambiando muchos de los procesos que actualmente conocemos y desarrollamos a diario y que sin duda irá ocupando un lugar más importante en nuestras vidas porque sus funciones son de gran valor para una población que está conectada a internet todo el día, que viaja por todo el mundo por ocio, trabajo, salud..., que cada vez dispone de menos tiempo libre o que simplemente se ha acomodado y necesita de unos servicios más rápidos y cómodos en todos los sentidos.

Por todo esto, pensamos que blockchain es una tecnología muy interesante para las AAPP, que va a ofrecer muchas oportunidades en un futuro cercano y que va a ayudar a estas a ofrecer unos servicios mucho mejores y con un menor coste para todos los contribuyentes, aspecto muy importante para cualquier sociedad.

La cadena de bloques será parte de nuestras vidas antes de que nos demos cuenta.

## Bibliografía

- Academy by Bit2me. *Smart Contracts: ¿Qué son. cómo funcionan y qué aportan?* s.f. <https://academy.bit2me.com/que-son-los-smart-contracts/> (último acceso: 22 de Mayo de 2019).
- Allende López, Marcos. «Blockchain: Cómo desarrollar confianza en entornos complejos para generar valor de impacto social.» Junio de 2018. <https://publications.iadb.org/es/publicacion/17379/blockchain-como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de> (último acceso: 4 de Abril de 2019).
- Ast, Federico, entrevista de Blockchain España. *El nacimiento de la justicia descentralizada con blockchain* Madrid, (10 de Abril de 2019).
- BBVA. *¿Cuál es la diferencia entre una DLT y blockchain?* 26 de Abril de 2018. <https://www.bbva.com/es/diferencia-dlt-blockchain/> (último acceso: 29 de Julio de 2019).
- Berryhill, J, T. Bourgery, y A. Hanson. "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", *OECD Working Papers on Public Governance, No. 28*. 2018. <<https://doi.org/10.1787/3c32c429-en>> (último acceso: 5 de Marzo de 2018).
- Corporation, Medium. *Aplicaciones del blockchain en el sector público*. 08 de Diciembre de 2018. <https://medium.com/@eraser/aplicaciones-de-blockchain-en-el-sector-p%C3%BAblico-885d7fda3023> (último acceso: 18 de Abril de 2019).
- . *Kleros, un Protocolo de Justicia para Internet*. 20 de Septiembre de 2017. <https://medium.com/kleros/kleros-un-protocolo-de-justicia-para-internet-920c28a588f1> (último acceso: 10 de Mayo de 2019).
- CRIPTONOCIAS. *¿Qué es la tecnología de contabilidad o blockchain?* s.f. <https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribuida-blockchain/> (último acceso: 02 de Abril de 2019).
- Escudero, José Luis. *Así funciona el sistema electoral español: la Ley D'Hondt y todas las claves del recuento del 20D*. 12 de Diciembre de 2015. <https://ecodiario.economista.es/elecciones-2015-20D/noticias/7215490/12/15/Asi-funciona-el-sistema-electoral-espanol-la-Ley-DHondt-y-todas-las-claves-del-recuento-del-20D.html> (último acceso: 24 de Julio de 2019).
- Español, Crypto & Blockchain en. *Prueba de trabajo (Pow) vs. Prueba de Participación (PoS)*. 18 de Septiembre de 2018. <https://medium.com/@cryptoblockchainespanol/prueba-de-trabajo-pow-vs-prueba-de-participaci%C3%B3n-pos-e99646d99483> (último acceso: 20 de Mayo de 2019).
- Ethereum. *El "Gas" en Ethereum*. 2018. <https://www.miethereum.com/ether/gas/> (último acceso: 25 de Mayo de 2019).

- FinTech. *Bosch, Cisco y otras empresas destacadas crean un consorcio de blockchain para el Internet de las cosas*. 30 de Enero de 2017. <https://www.fintech.es/2017/01/consorcio-de-blockchain-para-el-internet-de-las-cosas.html> (último acceso: 23 de Julio de 2019).
- García Mateo, P. *Blockchain aplicado al sector público*. Trabajo de Fin de Máster, Universidad Politécnica de Valencia, 2018.
- Jimenez, Javier Díaz. *¿Qué es Ethereum?: la apuesta por los contratos inteligentes*. 27 de febrero de 2018. <https://www.bbva.com/es/ethereum-que-es-contratos-inteligentes/> (último acceso: 24 de Mayo de 2019).
- Laguna, Pilar. *Blockchain: de la criptomoneda al criptopaciente*. 1 de octubre de 2018. <https://www.diariomedico.com/tecnologia/blockchain-de-la-criptomoneda-al-criptopaciente.html> (último acceso: 31 de Julio de 2019).
- Maldonado, Jose. *Votaciones Blockchain: mitos, realidades y retos futuros*. 28 de Mayo de 2019. <https://www.bitcobie.com/votaciones-blockchain-mitos-realidades-y-retos-futuros/> (último acceso: 25 de Julio de 2019).
- Merchan, Montaña. *Estrategia del Govern en Blockchain*. 19 de Junio de 2019. <https://digitalrevolution.info/2019/06/19/estrategia-del-govern-en-blockchain/> (último acceso: 27 de Julio de 2019).
- Noah, Emmanuel. *BenBen*. 04 de Abril de 2018. <https://www.solutions-summit.org/innovation/benben> (último acceso: 10 de Julio de 2019).
- Observatorio Blockchain. *Blockchain y la imparable transformación del sector energético mediante la eliminación de intermediarios*. 23 de Julio de 2019. <https://observatorioblockchain.com/blockchain-y-el-imparable-camino-del-sector-energetico-hacia-la-eliminacion-de-intermediarios/> (último acceso: 20 de Agosto de 2019).
- Pollock, Darryn. *El experimento Blockchain del Gobierno de Singapur es un camino hacia la comprensión normativa*. 20 de febrero de 2018. <https://es.cointelegraph.com/news/singapores-government-blockchain-experiment-is-a-road-to-regulatory-understanding> (último acceso: 30 de julio de 2019).
- PwC España. *Blockchain toma cuerpo entre las grandes empresas: 4 de cada 5 directivos asegura tener iniciativas en marcha*. 2018. <https://www.pwc.es/es/sala-prensa/notas-prensa/2018/blockchain-grandes-empresas.html> (último acceso: 03 de Mayo de 2019).
- Stone, Jeremy, entrevista de Susana Blázquez. *¿Cómo salvará Blockchain al sistema sanitario?* (11 de diciembre de 2018).
- TIVI. *TIVI: votación verificable accesible, en cualquier momento y en cualquier lugar*. s.f. <https://tivi.io/> (último acceso: 8 de Agosto de 2019).