# TEMA 106. LAS TECNOLOGÍAS EMERGENTES (BLOCKCHAIN). CONCEPTO. CLASIFICACIÓN, ASPECTOS JURÍDICOS Y APLICACIONES.

## ÍNDICE

# 1. TECNOLOGÍAS EMERGENTES. CONCEPTO. CLASIFICACIÓN, ASPECTOS JURÍDICOS Y APLICACIONES.

## 1.1. INTRODUCCIÓN

En el marco del conocido como ciclo de vida de las tecnologías (o también grado de madurez de las tecnologías) las tecnologías emergentes **son el primer escalón** que representa la aparición de una nueva tecnología. Las **siguientes fases** de este ciclo de vida corresponden a las tecnologías en **crecimiento**, las que ya son **maduras**, y las que se encuentran en **declive o saturación** (porque ya han aparecido otras tecnologías emergentes que las amenazan en términos de costes, eficacia, etc.).

**Tecnologías emergentes** son aquellas tecnologías innovadoras y disruptivas que pueden tener la **capacidad de crear nuevas industrias o transformar significativamente alguna ya existente**; también se suelen caracterizar por su **elevado grado de incertidumbre** dado que se encuentran en una etapa en la que aún no es evidente si habrá mercado para las mismas o si realmente se producirá un uso masivo de ellas. Así, en esta etapa suelen aparecer **debates** en torno a si estas tecnologías realmente tienen el potencial de cambio y empuje que se les anticipa desde varios ámbitos (económicos, tecnológicos, políticos, éticos, etc.).

Algunas de estas tecnologías ya son tratadas en otros temas del temario, tales como la **Inteligencia Artificial** (tema: "*Inteligencia artificial: la orientación heurística, inteligencia artificial distribuida, agentes inteligentes*"), el **Big Data** (tema: "*Big Data. Captura, análisis, transformación, almacenamiento y explotación de conjuntos masivos de datos. Entornos Hadoop o similares. Bases de datos NoSQL"*), el **Cloud Computing** (tema: "*Cloud Computing. IaaS, PaaS, SaaS. Nubes privadas, públicas e híbridas"),* el **Internet de las Cosas y las Ciudades inteligentes** (tema: "*La transformación digital e industria 4.0: ciudades inteligentes. Internet de las Cosas (IoT)*") o el **Data Mining** (tema: "*Gestión de los datos corporativos. Almacén de datos (Data-Warehouse). Arquitectura OLAP. Minería de datos*"). Por ese motivo, esta primera edición de este capítulo va a profundizar en la denominada tecnología Blockchain dado que **no existe un tema que la contenga** y a que en los últimos tiempos ha adquirido una **enorme relevancia en diversos ámbitos, tanto en el sector privado como en el público.**

**Comenzaremos explicando los orígenes** de la tecnología blockchain en su primera aplicación en el ámbito de las **criptomonedas**, centrándonos en bitcoin y su funcionamiento. Este enfoque nos ayudará a comprender algunas de sus principales características y cómo puede aplicarse blockchain a otros casos de uso diferentes de las criptomonedas tanto en el sector privado como en el público, donde veremos algunos proyectos que ya están en marcha usando esta tecnología. Finalmente veremos algunos aspectos jurídicos relacionados con blockchain.

Hoy por hoy, en el ámbito de la oposición, y dada la nueva estructura ministerial que se ha producido en febrero de 2020, con la creación de un **Ministerio de Asuntos**

**Económicos y Transformación Digital**, una de cuyas secretarías de estado se denomina **Secretaría de Estado de Digitalización e Inteligencia Artificial**, con **foco en la inteligencia artificial y otras *tecnologías habilitadoras***, podría pensarse que las tecnologías emergentes van a ser uno de los focos de interés de los próximos años. Por ese motivo, no está de más anticipar que **en el primer examen tipo test pueda aparecer alguna pregunta relacionada con este tema**, del mismo modo que conviene conocer el entorno de esta tecnología blockchain para, llegado el caso, justificar o no en un supuesto práctico, el empleo de la misma como parte de la solución propuesta.

# 2. BLOCKCHAIN

## 2.1. INICIO DE BLOCKCHAIN

Una de las aplicaciones más famosas de la tecnología blockchain es el **bitcoin** y el resto de criptomonedas que existen. La tecnología que subyace a bitcoin es blockchain, y **es importante distinguir que las criptomonedas son solamente una de las posibles aplicaciones de la misma**. Desde hace varios años se están encontrando aplicaciones de estas tecnologías en otros muchos ámbitos. **La proliferación de casos de uso en diversos sectores es extraordinaria** e incluso **las Administraciones Públicas se encuentran explorando** la posibilidad de implementar casos de uso utilizando esta tecnología; en algunas de ellas ya existen proyectos en marcha basados en blockchain como veremos más adelante.

Aunque con anterioridad al nacimiento de bitcoin ya existían publicaciones sobre la tecnología blockchain[1], la explosión de blockchain se encuentra ligada al nacimiento de bitcoin en 2008 en el famoso artículo[2] de Satoshi Nakamoto[3] (pseudónimo de su autor o autores), quien creó esa criptomoneda en 2009; con ello, dio lugar al denominado "Internet del valor", dado que **blockchain posibilita la transferencia de valor en Internet entre dos partes sin necesidad de intermediarios o terceras partes**. Por ese motivo, **blockchain suele encontrar aplicaciones en entornos donde no existe confianza entre los actores que participan**.

[1] *Habber, W.S. Stornetta – "How to time-stamp a digital document", 1991*
[2] *Nakamoto, Satoshi "Bitcoin P2P e-cash paper", 1 de noviembre de 2008.*
[3] *En su honor se denomina 'Satoshi' a la cienmillonésima parte de un bitcoin.*

## 2.2. EXPLICACIÓN DE BLOCKCHAIN

**Blockchain es un registro distribuido entre los diversos participantes (nodos) de una red, cada uno de los cuales posee una copia completa de ese registro.** Como tal registro (*ledger* en inglés) consiste en un **listado de apuntes, de transacciones, de hechos**…, en definitiva, de eventos que han ocurrido (tales como transferir dos bitcoin de Marta a Juán; o que una universidad haya emitido un diploma académico a María; o que Antonio haya obtenido su carné de conducir; o que haya llovido). **La ocurrencia de un evento es trasmitida (*broadcast*) al conjunto de la red** de forma que **todos los participantes (nodos) tengan conocimiento de que ese suceso ha tenido lugar** realmente **y cada uno de ellos lo registre en su copia local.**

Un **nodo** puede consistir en un **ordenador, un teléfono móvil, un conjunto de servidores, etc...,** cualquier sistema informático en donde se pueda ejecutar el **software** que permite participar en una red de blockchain.

**El registro se divide en bloques**, cada uno de ellos con un **tamaño máximo predefinido** o acordado de antemano de manera que, **cuando un bloque se termina de escribir** con las anotaciones de los eventos que han ido sucediendo hasta entonces, se aplica un ***algoritmo de consenso,*** el cual es la forma en que **los nodos de la red acuerdan entre ellos que lo escrito en ese bloque ha ocurrido realmente**. De este modo se produce consenso en torno a lo que cada uno de los nodos ha ido escribiendo a medida que los eventos se sucedían, esto es: **han observado la misma realidad**. Por ejemplo, en el algoritmo de consenso utilizado en bitcoin, al menos el 50% de los nodos han de encontrarse de acuerdo en que han escrito un bloque que contiene las mismas transacciones (aunque no se encuentren necesariamente en el mismo orden).

Existe una **gran variedad de algoritmos de consenso** que se aplican en función de varios parámetros tales como el nivel de confianza entre los participantes, el tipo de red blockchain, etc. Más adelante explicaremos los algoritmos de consenso más relevantes.

Una vez se produce ese consenso, **todos los nodos de la red** (los cuales se comunican entre sí a través de protocolos *Peer-to-Peer* – P2P) **copian localmente ese bloque consensuado**. **De este modo se garantiza que la copia en cada nodo es idéntica a la de los demás nodos sin existir una autoridad central que coordine esa copia**. A continuación comienza a escribirse un **nuevo bloque**, el cual siempre **comenzará en su cabecera con el resultado de aplicar una función *hash* (típicamente SHA-256) calculado a partir de toda la información contenida en el bloque anterior.** Por ese motivo se habla de ***cadena de bloques* o blockchain** puesto que cada bloque se encuentra intrínsecamente ligado al bloque anterior mediante esa función hash siguiendo lo que se conoce como estructura de árbol de Merkle, lo cual permite verificar con facilidad que grandes estructuras de datos no han sido modificadas.

En el protocolo P2P **los nodos se conectan por parejas**, a su vez los nodos no están conectados todos entre sí, sino que cada uno de ellos lo está con un número

determinado a los cuales transmite información y estos a su vez la retransmiten a aquellos otros a los que éstos se encuentran conectados, y así sucesivamente hasta que la información se propaga a todos los nodos de la red.

Esta tecnología se engloba dentro de las denominadas como tecnologías DLT (*Distributed Ledger Technologies)*, en las cuales puede no ser necesaria la característica de inmutabilidad propia de blockchain.

## 2.3. CARACTERÍSTICAS DE BLOCKCHAIN

Algunas consecuencias de esta estructura son:

### 2.3.1. Descentralización de la información.

Toda la información se encuentra replicada en cada uno de los nodos participantes, los cuales pueden encontrarse repartidos por todo el globo y hacer imposible controlar la información del registro a ningún país, organización o individuo. Por tanto **no existe ninguna autoridad centralizada que controle la información**.

### 2.3.2. Inmutabilidad.

Una vez escrito un bloque en la cadena es imposible modificar ninguna de la información que contiene, dado que ya no coincidiría su *hash* con el que se encuentra escrito en el cabecero del bloque siguiente. En todo caso sólo es posible añadir más información en los bloques siguientes.

### 2.3.3. Transparencia.

Derivada del consenso necesario para escribir nuevos bloques y el hecho de que sea necesario alcanzar acuerdos. Todos los nodos de la red poseen una copia local idéntica de la información, de toda la cadena de bloques y cualquiera puede acceder a esa información. Esto permite también que la información sea trazable y sea posible conocer los diversos estados por los que ha ido transitando un activo o información.

### 2.3.4. Transferencia de valor entre pares.

La autoridad central que generalmente atestigua que un evento se ha producido (por ejemplo una transferencia de valor entre dos partes) es sustituida en blockchain por todos los nodos de la red, **los cuales son testigos de que dicha transacción ha tenido lugar**. Además, antes de escribir un nuevo bloque han de acordar entre ellos que efectivamente han presenciado ese conjunto de eventos anotado en ese bloque y que ese evento es posible según unas reglas predefinidas.

### 2.3.5. Seguridad.

El hecho de que **toda la cadena de bloques se encuentre replicada en cada nodo** hace muy **difícil la manipulación de la información ante ataques**. En caso de que intente añadirse a la red por parte de un nodo información que no ha ocurrido o es falsa, **ésta simplemente se ignora o se rechaza**. Esta estructura también permite que **la caída o mal funcionamiento de uno de los nodos no afecte a la información de la red dado que el resto de nodos posee una copia completa de la misma**. También proporciona una **alerta temprana ante ataques**, ya que el resto de nodos detectan que en uno de ellos se produce un cambio. Por su parte**, la forma en que cada bloque está conectado con el anterior** a través de una función *hash* le da una **capa de seguridad** adicional e integridad a la cadena de bloques. **Por último**, aparece otra capa más de seguridad en el método que se escoge para elegir cuál será el nodo que escriba el bloque siguiente, el conocido como **algoritmo de consenso**.

### 2.3.6. Ausencia de jerarquía.

Todos los nodos de la red se encuentran al mismo nivel jerárquico que los demás ya que la toma de decisiones respecto a la escritura de información se produce en base al algoritmo de consenso elegido.

## 2.4. FUNCIONAMIENTO DE BITCOIN

Explicaremos en primer lugar el funcionamiento básico de bitcoin (que es esencialmente el mismo en el resto de criptomonedas) que nos ayudará a entender más adelante otro tipo de aplicaciones de blockchain distintas de las criptomonedas.

**Bitcoin es una red abierta, pública o no permisionada**, esto significa que no es necesario obtener permiso de ninguna autoridad para operar en la misma, cualquiera puede descargarse el software necesario y la cadena de bloques completa para operar en la red y convertirse en un nodo más, por ese motivo **el grado de confianza entre los participantes** de este tipo de **redes es mínimo ya que no se conocen entre sí.**

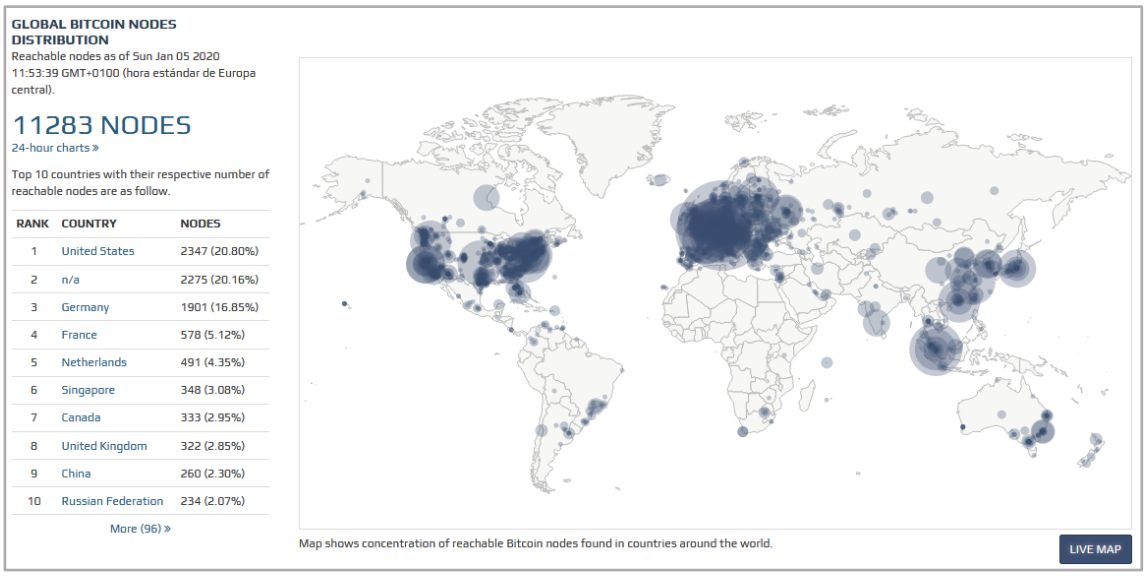



*Ilustración 1. Distribución de nodos activos en bitcoin. Fuente: bitnodes.earn.com*

**La blockchain de bitcoin** (o de cualquiera de las demás criptomonedas existentes) **es el registro de las transacciones de bitcoins que se producen entre las personas a través de Internet**. Para conocer el saldo en bitcoins de cualquiera de los usuarios de la red, **es necesario leer todos los bloques de la cadena**, en orden secuencial desde el primero hasta el último, de esta forma es posible leer el registro de operaciones en las que un usuario ha intervenido para conocer su saldo final simplemente realizando operaciones de suma y resta. Por ese motivo **el orden de los bloques** que ofrece blockchain mediante el método de los hashes **es muy importante** ya que nos da la secuencia temporal e inalterable de transacciones. Esto permite también evitar que un usuario transfiera más bitcoins de los que posee, del mismo modo que ocurre cuando quien realiza esa gestión es un banco en un modelo centralizado.

**En bitcoin el algoritmo de consenso es del tipo de los denominados "prueba de trabajo" (*Proof of Work* – PoW).** En este tipo de algoritmos el bloque siguiente a escribir en la cadena es propuesto por **aquel nodo que resuelva un problema matemático** computacionalmente complicado. Por este motivo a los nodos en bitcoin se les denomina también "**mineros**" dado que han de trabajar intensamente para resolver ese problema matemático, tan difícil, **que el azar juega un papel muy importante**. **Los mineros en bitcoin compiten entre sí** intentando resolver ese problema, dado que aquel minero que lo resuelva recibe una sustancial recompensa en forma de bitcoins que a día de hoy es de **12,5 bitcoin** (unos 83.500 euros al cambio actual). Esta recompensa va

reduciéndose paulatinamente (en 2009 eran 50 bitcoin), de hecho esta es la forma en que se crean los bitcoins, a través de estos pagos que el sistema hace a un minero cuando encuentra la solución al problema, cosa que ocurre aproximadamente cada 10 minutos. Así se consigue que los bitcoins se repartan de manera aleatoria entre todos los nodos de la red evitando que se encuentren en poder de los mismos usuarios. Los mineros también pueden recibir pagos adicionales en forma de comisiones sobre las transacciones, las cuales pagan los usuarios que ordenan esas transacciones; a su vez estas comisiones también son un incentivo para que el minero incluya esas transacciones en el bloque.

A este proceso de reducción paulatina de la recompensa con el tiempo a los mineros se le denomina "***halving***" y hace que la tasa de creación de bitcoins se reduzca paulatinamente hasta que se alcance la cantidad máxima de bitcoin que existirán en circulación, cantidad que está predeterminada de antemano en **21 millones de bitcoins**. Esa cifra se alcanzará **en el año 2140** y **la recompensa que obtienen los mineros se divide por la mitad cada 210.000 bloques**, **cosa que ocurre aproximadamente cada cuatro años**, por lo que **en el año 2140 los mineros únicamente obtendrán las comisiones por las transacciones**. El *halving* es uno de los elementos fundamentales del funcionamiento económico de las criptomonedas, ya que con este método se procura que **el tipo de modelo monetario sea deflacionario**, esto es, **que la moneda aumente su valor con el tiempo de manera controlada.**

**La primera transacción del bloque siguiente reflejará este pago que la red efectúa al minero que ha vencido en la prueba.** Este premio es el incentivo que tienen los mineros para trabajar en el proceso que se conoce como "**minado de bloques**".

**Puesto que se trata de un problema de muy alta dificultad, en principio cualquiera de los mineros es susceptible de resolverlo**, por esto insistimos en que el azar tiene una componente importante a la hora de determinar quién se lleva el premio. Con este sistema, y dado el gran número de mineros existentes, **es muy difícil que la escritura de bloques sea controlada por la misma entidad** así como evita que **haya dos bloques escritos a la vez (que se produzcan colisiones de escritura) con información contradictoria sin que exista una autoridad central que coordine el proceso**, ya que quien propone el nuevo bloque es el minero que ha resuelto el problema y es muy improbable que dos mineros encuentren al mismo tiempo una solución.

A continuación describimos la estructura básica de un bloque de la cadena, información que todos los mineros van escribiendo localmente a partir de información que calculan, observan y procesan, conteniendo la siguiente información resumida:

### 2.4.1. Cabecera.

Contiene **el *hash* calculado** sobre la totalidad del bloque anterior.

### 2.4.2. Transacciones.

Las cuales va recibiendo (observando) y anotando cada minero, al tiempo que también realiza comprobaciones sobre la validez de esas transacciones. Los usuarios poseedores de bitcoin realizan pagos entre ellos, esas transacciones se comunican a los nodos mediante un ***broadcast*** de modo que la información se transmite mediante un protocolo P2P a todos los nodos (mineros) de la red. **Cada minero posee una copia completa de la cadena de bloques** y **puede comprobar si esas transacciones son válidas** (por ejemplo comprobando que los usuarios tienen saldo suficiente para transferir los bitcoins que desean y en definitiva que la nueva información a añadir no entra en conflicto con la ya existente en la red de blockchain).

### 2.4.3. NONCE.

**Cuando en un bloque se alcanza una cierta capacidad (unas 1800 transacciones de media a día de hoy[4], número que puede llegar hasta unas 3500 transacciones que alcanzarían el límite máximo de 1 MB permitido por bloque)** los mineros añaden el denominado **NONCE** (*'number that can be only used once'* o número que solo puede usarse una vez), un **valor arbitrario** tal que al aplicar la función *hash* al conjunto del bloque (incluyendo el NONCE) el *hash* resultante comienza por 32 ceros: ese es el difícil problema a resolver y solamente puede hacerse aplicando fuerza bruta, esto es, de los 256 bits de que consta el *hash* SHA-256, los primeros 32 han de ser ceros. El número de ceros no es casual, es el que permite que el problema sea resuelto aproximadamente cada 10 minutos y este número de ceros ha ido aumentando con el tiempo. En caso de que ese intervalo de tiempo promedio bajara significativamente de 10 minutos (porque la capacidad de computación haya aumentado) entonces se añadiría un cero más al problema aumentando su denominado *grado de dificultad*. **En bitcoin el grado de dificultad se ajusta cada 2016 bloques (unas dos semanas) procurando que los bloques tengan un tiempo de minado promedio de 10 minutos. Cada criptomoneda fija su grado de dificultad propio**, así en la criptomoneda **ethereum** el grado de dificultad es de alrededor de **20 segundos**[5]. La dificultad del problema en bitcoin es tal que a día de hoy (enero de 2020) la capacidad de computación es de **casi 120 Terahashes por segundo con el subsiguiente enorme gasto energético que esto conlleva**. Por ese motivo existen

[4] https://www.blockchain.com/es/charts/n-transactions-per-block?timespan=all
[5] Fuente: https://etherscan.io/chart/blocktime

granjas de servidores dedicadas exclusivamente al minado de bloques en bitcoin que suelen localizarse en países donde el coste energético es menor o en lugares caracterizados por climas con bajas temperatura para reducir los costes de refrigeración de los servidores.

En este proceso de minado, **el minero que consigue resolver el problema transmite la solución al resto de mineros de la red**, los cuales **comprueban** que **la información de ese bloque es válida** (el cálculo del ***hash*** del **bloque anterior**; comprueban la **validez de las transacciones** y comprueban que el **NONCE propuesto por ese minero resuelve el problema descrito**). **Si más del 50% de los mineros aceptan ese bloque como válido tras las comprobaciones, entonces ese bloque pasará a ser el definitivo** de la cadena de bloques y copiado a todos los nodos de la red comenzando el proceso de nuevo.

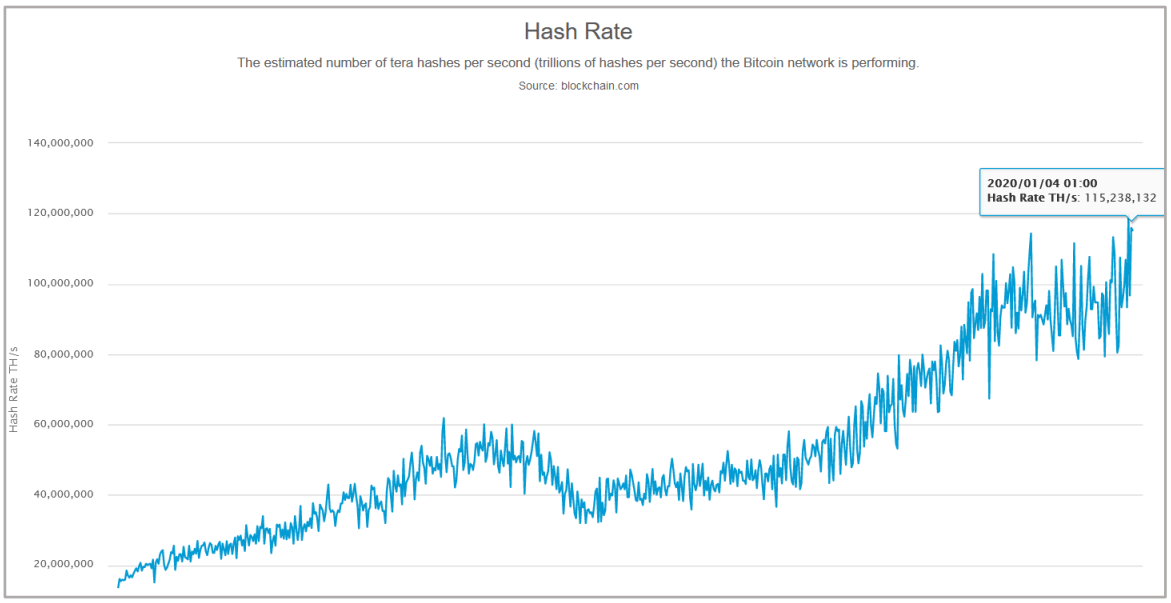



*Ilustración 2. Tasa de hashes calculados por segundo. Fuente: https://www.blockchain.com/es/charts/hash-rate*

## 2.5. WALLET O MONEDEROS

Los usuarios poseedores de criptomonedas necesitan instalar un **programa informático** que se denomina *wallet* (traducido a veces como **monedero** y a veces como **llavero**). Existe una **gran proliferación de empresas** que a día de hoy desarrollan este tipo de programas informáticos. En el caso de las criptomonedas la función principal del *wallet* consiste en **gestionar un par de claves criptográficas asimétricas**, cu**stodiando la clave privada y publicando en blockchain la clave pública**. Esta última se encuentra **en una determinada (y única) dirección de blockchain,** de manera que así e**s posible demostrar que el poseedor de la clave privada es quien controla esa dirección en blockchain y por tanto es el dueño de los bitcoins asociados a esa dirección.**

Las anotaciones en el registro de blockchain se refieren a operaciones realizadas por esas direcciones, las cuales son controladas por los *wallets* y así **se impide conocer la**

**identidad real del usuario que controla esa dirección**; no obstante **sí que es posible conocer todos los movimientos asociados a una dirección determinada**. Este anonimato asociado a la red bitcoin ha **facilitado** que esta criptomoneda se utilice de **entornos delictivos**.

A la hora de realizar una operación en bitcoin, los usuarios **firman** la transacción **con su clave privada**, lo que demuestra que son los dueños de los bitcoin asociados a la transacción. Esto es algo que **cualquiera puede comprobar** utilizando la clave pública que se encuentra almacenada precisamente en esa dirección de blockchain.

**Los *wallet* se pueden instalar en un dispositivo local o bien en la nube**, y no solamente sirven para almacenar las claves, sino que **en aplicaciones de blockchain más allá de las criptomonedas**, también sirven para **almacenar credenciales** de los usuarios como veremos en un apartado más adelante.

## 2.6. TIPOS DE CRIPTOMONEDAS

En la actualidad existen alrededor de **2.500 criptomonedas diferentes**[6], y el número parece que sigue aumentando, fundamentalmente debido al gran auge de las **ICO** (*Initial Coin Offering*) las cuales consisten en adquirir criptomonedas por parte de inversores iniciales en nuevos negocios o proyectos que les darán derechos sobre esos negocios o proyectos.

En este punto conviene introducir el concepto de ***token*** como una **representación visible o tangible de un objeto, hecho, calidad, cualquier valor, etc.** En el mundo virtual, los *tokens* **representan un activo que puede consumirse o comercial con él.** Al igual que las criptomonedas, **se encuentran representados en redes de blockchain**, las cuales ya hemos insistido que determinan y **transmiten valor entre partes**, **cualquier tipo de valor**, y una de las formas de representar este valor son los *token*. Hay diferentes tipos de *token* en función de la aplicación para la que hayan sido diseñados.

Un posible modo de **clasificar** los **diferentes tipos de criptomonedas** que existen radica en el **uso** que se les puede dar, y aquí hay que incluir este concepto de *token*. De este modo, y atendiendo a un criterio funcional, podemos encontrar las siguientes agrupaciones:

[6] https://coinmarketcap.com/

### 2.6.1. Criptomonedas que poseen valor intrínseco.

Su **uso es el mismo que el del dinero**, que las divisas, y permiten adquirir bienes y servicios de todo tipo. Su valor lo otorga el mercado y no son gestionadas por autoridades centrales (bancos, estados, etc.), tampoco tienen fronteras ni jurisdicciones ya que han aparecido en un entorno global. El paradigma de este caso es el bitcoin.

### 2.6.2. "Utility tokens" o monedas de utilidad.

En este tipo de redes blockchain, **lo que interesa** no es la moneda en sí sino **la información que se almacena en la red**. Este tipo de criptomoneda se utiliza **para pagar servicios relacionados con la información almacenada en esas redes**, esto es, le ofrece al usuario la **capacidad de utilizar un producto o servicio determinado**.

Típicamente se trata de **empresas que** en una red **blockchain desarrollan productos o servicios digitales y venden este tipo de *tokens*** a los usuarios, quienes a su vez, pueden utilizarlos para comprar diferentes servicios en la aplicación **del mismo modo que si se tratara de cupones**. Por ejemplo un *token* "alojamiento en casa rural" podría utilizarse para pagar una estancia de fin de semana en una casa rural al dueño del alojamiento.

Este tipo de criptomonedas también **suelen aparecen ligadas al concepto de "*smart contract*"**, los cuales, como veremos más adelante, **son programas informáticos, algoritmos, que se encuentran escritos en un blockchain (por tanto son inmutables)** y condicionan las transacciones que se producen en la red. Esos programas **requieren capacidad de ejecución que tiene un coste asociado** por lo que **las criptomonedas** en esta categoría **sirven para pagar esa capacidad de ejecución**. El ejemplo más relevante de este tipo es ***ethereum***, un tipo de criptomoneda que se puede utilizar para comprar "gas" que a su vez proporciona poder de cómputo en este tipo de redes blockchain.

### 2.6.3. "Security token" o monedas de titularidad.

Este tipo de *token* **representa la propiedad de un activo digital en redes blockchain (títulos de activos).** El activo digital puede referirse a **activos materiales y no materiales** de la vida real (por ejemplo, bienes inmuebles o acciones de una empresa). **Debido a que estos tokens se consideran de titularidad, están sujetos a regulación**, por lo que **en algunos países se tratan de la misma manera que los valores tradicionales.**

A su vez se pueden distinguir tres tipos en esta categoría:

- **Acciones**. Las participaciones de los socios en una empresa pueden convertirse en partes (*tokens* o representaciones de un activo) y a continuación repartir esos *tokens* entre los socios, todo ello en una red de blockchain. Los

propietarios de esos *tokens* pueden a su vez venderlos a terceros. En este grupo es donde han proliferado muchas de las ICO que han ido apareciendo, también es donde ha aparecido una gran cantidad de fraude asociado a estas participaciones.

- **Deuda**. El mismo concepto aplicado al caso de una deuda. El agente emisor de la deuda puede dividirla en *tokens* que adquieren un derecho sobre esa deuda y el poseedor de esos *tokens* también se convierte en titular de la deuda.
- **Activos físicos**. Típicamente inmobiliarios, pero su utilidad se extiende a todo tipo de activos. Como en los casos anteriores consiste en transferir el valor de un activo físico a *tokens*, de este modo el poseedor de esos *tokens* es el dueño del activo físico (una casa, un vehículo, una finca, etc.).

**A menudo es difícil distinguir si nos encontramos ante una criptomoneda de utilidad o de titularidad,** por eso se ha definido el denominado "**Test de Howey**" a partir de una sentencia de un tribunal de Estados Unidos para determinar si cierto acuerdo implicaba un contrato de inversión y nos encontramos ante un instrumento financiero, en cuyo caso el regulador ha de supervisar esta inversión. Según este test, nos encontramos ante una criptomoneda de utilidad si se cumplen las siguientes características:

- Ha de haber inversión de dinero.
- Hay expectativas de obtener beneficios.
- La inversión ha de hacerse en una empresa común.
- Los beneficios se derivan predominantemente de los esfuerzos de terceros y no dependen del control del inversor.

## 2.7. TIPOS DE REDES BLOCKCHAIN

**Existen fundamentalmente tres tipos de redes blockchain, las redes públicas, las redes privadas y las redes híbridas** que son al mismo tiempo públicas y permisionadas. En función del tipo de red que se trate, el funcionamiento de la misma y el tipo de algoritmo de consenso tenderá a ser de uno u otro tipo como ver**e**mos más adelante. las redes públicas, las redes privadas y las redes híbridas

### 2.7.1. Blockchain públicas.

Son **redes completamente descentralizadas** accesibles desde Internet y en donde **cualquiera puede descargarse el software** necesario para operar incluso como nodo **sin ninguna restricción ni necesidad de permiso**. También es posible hacerse con una copia

de la cadena de bloques para estudiarla, auditarla, analizarla,… Uno de los ejemplos más relevantes de este tipo de redes es el de bitcoin y otras muchas criptomonedas. En ellas el algoritmo de consenso se basa en la minería y requiere de un alto poder computacional. Generalmente los **usuarios** en estas redes son **anónimos** y se encuentran al mismo nivel, no existe ningún tipo de jerarquía.

### 2.7.2. Blockchain privadas o permisionadas.

Como su nombre indica **es necesario obtener un permiso para formar parte de la red** en forma de nodo o para acceder a la información contenida en el blockchain. Por tanto no se trata de redes descentralizadas, dado que y son quienes otorgan el permiso para operar en la misma, también son quienes se encargan del mantenimiento de la red, de manera que en este tipo de redes sí existe una cierta jerarquía. **una entidad o grupo de entidades controla quienes son los participantes en la red** Generalmente **en estas redes se conoce la identidad de los intervinientes** y **suelen consistir en consorcios de empresas que necesitan compartir información entre ellas,** por lo que **no es necesario un alto coste** computacional al encontrar formas de consensuar la información mucho más sostenibles que los algoritmos de consenso basados en fuerza bruta, siendo además redes más eficientes. Algunos ejemplos son Hyperledger (iniciado por la Fundación Linux), Corda (de R3), Ripple, Quorum (de JP Morgan) o Chain.

### 2.7.3. Blockchain híbridas (públicas y permisionadas).

Son **una combinación de las dos anteriores**, así **para** poder **actuar como nodo** e inyectar información en el blockchain **es necesario obtener un permiso y conocer su identidad real**, no obstante **son también públicas** en el sentido de que **cualquiera puede acceder y consultar la información publicada en la cadena de bloques.** Se considera que este tipo de red es **la idónea en proyectos blockchain** donde **administraciones públicas** ofrezcan servicios a los ciudadanos, siendo también redes muy sostenibles desde el punto de vista energético. Ejemplos de estas redes son BigchainDB, Evernym, Quorum en el consorcio Alastria[7] en España o *la European Blockchain Services Infrastructure* que veremos más adelante.

[7] Consorcio de más de 500 empresas pertenecientes a múltiples sectores que colaboran para crear un ecosistema de servicios basados en blockchain y cuyo pilar fundamental es su modelo de identidad digital autogestionada. *https://alastria.io/*

## 2.8. ALGORITMOS DE CONSENSO

**En las redes distribuidas donde no existe una autoridad central ni terceras partes** que organicen y coordinen los flujos de información, **un algoritmo o mecanismo de consenso es la forma en que se toma una decisión por parte de un grupo** formado por varios participantes que, **en** caso de **blockchain**, se refiere al procedimiento por el cual **se acuerda por los participantes cuáles son las transacciones que se van a escribir en el siguiente bloque.** También persigue que todos los integrantes de la red se encuentren en igualdad de condiciones (derechos) a la hora de participar en la misma y en su caso beneficiarse de ella. En redes distribuidas, estos algoritmos de consenso son el mecanismo que se utiliza para que la información en la red se conserve de forma segura e íntegra. **Son** por tanto, **uno de los pilares fundamentales donde descansa la seguridad de las redes blockchain.**

En estos **entornos distribuidos**, a menudo caracterizados por contener **grandes dosis de desconfianza**, y en donde **los implicados no se conocen entre** sí, es necesario establecer mecanismos que minimicen la posibilidad de que la red se corrompa ya sea porque algunos **participantes maliciosos** no siguen las reglas, por **mal funcionamiento de la red**, por **fallos de cualquier tipo, etc.** A este tipo de problemas se les denomina "**Problema de los Generales Bizantinos – BFT *(Bizantine Fault Tolerance)*"**[8], y aparece en varios escenarios que **requieren que la red en su conjunto ofrezca una respuesta ante la aparición de este tipo de fallos** que generalmente son muy difíciles de detectar, porque **no suele estar claro para distintos observadores que realmente haya un fallo en un componente del sistema**. En esos casos **se diseñan métodos para alcanzar acuerdos** sobre el correcto funcionamiento de la red para que el sistema pueda continuar funcionando y resistir este tipo de fallos denominados BFT.

El Problema de los Generales Bizantinos se puede resumir como sigue: un general de un ejército envía un mensajero a otros generales con un mensaje indicando el momento en que el ejército debe atacar. A su vez los generales que reciben y confirman el mensaje han de reenviarlo al resto de generales de manera que la información se conozca por todos ellos antes del ataque. El problema consiste en que el enemigo pudiera interceptar mensajeros y alterar los mensajes en su beneficio. Para evitarlo, todos los generales deberían poseer algún tipo de información que les permitiera reconocer si el mensaje original se ha alterado.

En el caso de las redes P2P, se diseñan algoritmos para que los integrantes de la red lleguen a un acuerdo respecto de si un componente está o no funcionando correctamente, o a si alguien está intentando inyectar información maliciosa en la red; con la dificultad añadida de que han de alcanzar un acuerdo en un entorno de alta desconfianza mutua. Los algoritmos de consenso consiguen también que todos los participantes de la red posean una copia idéntica del registro de blockchain.

[8] Leslie Lamport, Robert Shostak, and Marshall Pease. *"The Byzantine Generals Problem"*

Han surgido **gran cantidad de diferentes algoritmos de consenso** que se utilizan en diversos tipos de redes blockchain, **cada una de ellas elige el algoritmo que más se ajusta a sus intereses. Los más comunes son los denominados "Prueba de trabajo (Proof of Work – POW)" y "Prueba de Participación (Proof of Stake – POS).**

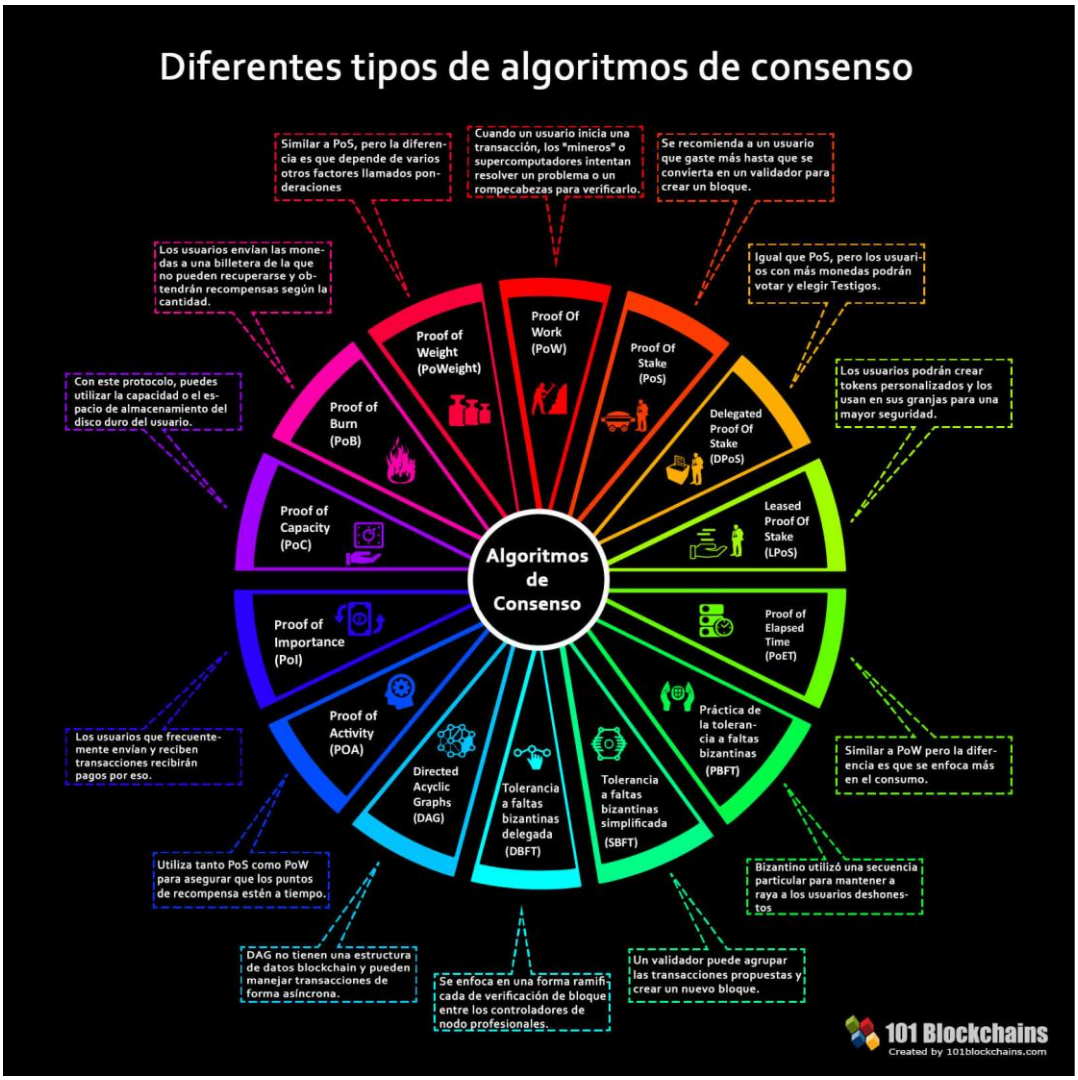



*Ilustración 3. Gran variedad de algoritmos de consenso. Fuente 101blockchains.com*

### 2.8.1. Proof of Work – PoW.

Es el algoritmo que **hemos descrito anteriormente** en el apartado de bitcoin y fue el primer algoritmo de consenso utilizado en el ámbito de blockchain. También es el algoritmo que se utiliza en otras **muchas criptomonedas**. La idea en la que se basa es la de resolver un **problema matemático complejo** (proceso denominado como ***minería***) que, por tanto, requiere de una **gran capacidad computacional**, lo que conlleva uno de

los grandes problemas de este sistema: el **desorbitante consumo de energía** que lo acompaña**. La confianza en este algoritmo descansa sobre la capacidad de trabajo.** Quien resuelve ese problema obtiene una **recompensa** y propone el contenido del bloque siguiente, por ese motivo un gran poder computacional aumenta las probabilidades de llevarse el premio y, por eso también ese poder computacional va aumentando paulatinamente, lo cual requiere que el problema tenga que ser cada vez más complicado**. Aunque la resolución del problema es muy difícil, en cambio comprobar que la solución es válida es muy sencillo**. Si más de la mitad de los nodos acuerdan que el contenido propuesto por el nodo ganador ha ocurrido realmente entonces ese bloque pasa a ser el siguiente de la red de bloques. Otro de los problemas a que se enfrenta este algoritmo es el conocido como "**Ataque del 51%"**, en el cual, **si una entidad concreta fuera capaz de controlar el 51% de los nodos entonces podría decidir qué información se escribe en el blockchain**, es por eso que **la seguridad de la red aumenta con el número de nodos que la componen.** También se considera que este algoritmo ofrece una alta resistencia ante ataques DOS (*Denial of Services*). El algoritmo de prueba de trabajo es el más utilizado en redes públicas tales como las utilizadas en las criptomonedas.

### 2.8.2. Proof of Stake – PoS.

El algoritmo "**prueba de participación"** apareció en 2011[9] como una **alternativa a PoW** intentando eliminar algunas de sus ineficiencias. En este **algoritmo no se resuelve ningún problema matemático**, por lo que es **mucho más sostenible** desde el punto de vista energético, en su lugar, **el nodo que propone el siguiente bloque** de la red **es elegido por un proceso pseudoaletorio que tiene en cuenta la cantidad de criptomonedas que posee** en su monedero el minero– que en este algoritmo recibe el nombre de ***validador*** –, **el tiempo que hace que las posee ("*staked*")** y l**a cantidad de las mismas que ha invertido en el proceso de minado para comprar mayor probabilidad de ser elegido y escribir el nuevo bloque**, **funcionando el proceso como una lotería**. **Esta inversión económica de los validadores se considera una garantía de que los mismos no van a actuar de forma maliciosa**, ya que si se detecta que una transacción no es válida entonces el nodo validador pierde sus fondos, en cambio, si actúa de forma correcta recibe una recompensa por validar las transacciones y crear nuevos bloques. Este algoritmo se basa en la asunción de quien posee más riqueza es el más indicado para protegerla y por tanto es en quien más se pueden confiar las tareas de validación, ahí es donde se sustenta la confianza en este algoritmo.

[9] Sunny King, Scott Nadal "*PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*"

Una de las consecuencias de este algoritmo es que **tiende a concentrar la riqueza entre unos pocos**, **que a su vez son los que escriben los nuevos bloques**. Las criptomonedas Peercoin, Blackcoin y NXT han sido algunas de las que comenzaron a utilizar este algoritmo, **recientemente la red Ethereum ha decido utilizarlo**. POS también se utiliza al igual que POW en varias criptomonedas (Peercoin, PIVX, NavCoin, ShadowCash Stratis, etc…) y también en redes privadas. El algoritmo requiere que la información contenida en los monederos de los validadores sea pública de forma que se pueda demostrar que efectivamente se poseen los fondos necesarios para participar en el sorteo.

Este algoritmo permite que el nivel de latencia de transacciones sea menor, por lo que es posible escribir un mayor número de bloques por unidad de tiempo, lo que permite una mayor escalabilidad y velocidad de la red sin necesidad de gran capacidad de cómputo.

### 2.8.3. Delegated Proof of Stake – DPoS.

El algoritmo de Prueba de Participación Delegada es **la variante más común a PoS** y **aumenta los niveles de escalabilidad de la red** sin requerir altos niveles de consumo energético. **También** es utilizado fundamentalmente **en redes públicas**. En este algoritmo **los nodos eligen por votación un conjunto de "delegados" en los que se deposita la confianza**, también se elige **el número concreto de delegados, y algunos aspectos relacionados con el funcionamiento de la red.** En esta votación sin requerir altos niveles de consumo energético. **se tienen en cuenta aspectos como la reputación** de los nodos y **el grado de participación** de los mismos en la red (número de *tokens* que poseen), **de ahí su relación con el algoritmo PoS**. A su vez los **nodos que han sido elegidos como delegados se organizan de manera que la escritura de nuevos bloques se realiza por turnos rotatorios**, en donde en cada turno ha de escribir un bloque un delegado concreto según un orden predeterminado y, en caso de no hacerlo (por encontrarse caído o por cualquier otra circunstancia), entonces ha de esperar una vuelta completa y su turno pasa al siguiente delegado. Los delegados reciben una recompensa al escribir nuevos bloques, aunque también **pueden ser** expulsados si se comprueba que la información que proponen escribir, una vez revisada, no se corresponde con lo observado por el resto. Algunas de las redes que utilizan este algoritmo son BitShare, EOS, Lisk, Ark, Steem, Cardano o Tron.

### 2.8.4. Proof of Authority – PoA.

El algoritmo conocido como **prueba de autoridad** se utiliza **fundamentalmente en redes permisionadas o privadas**, en las cuales todos los nodos poseen permiso para poder participar en la red. **Al igual que en DPoS**, estos nodos a su vez, **eligen un subconjunto de nodos validadores** que son los que pueden escribir nuevos bloques. En este algoritmo **la confianza se deposita en la reputación y la identidad real del nodo** que escribe un nuevo bloque (validador), **reputación que puede verse muy disminuida en caso de que el nodo tenga comportamientos inapropiados y sea expulsado**, por lo que le **conviene seguir las reglas.** La **escritura de nodos se realiza por turnos** de forma rotatoria en donde cada validador escribe un nuevo bloque en su turno. Este tipo de algoritmos permite altos niveles de escalabilidad sin necesidad de alto poder de cómputo. La red EBSI va a utilizar una variante de este algoritmo de consenso.

### 2.8.5. Practical Bizantine Fault Tolerance – PBFT

El objetivo del algoritmo PBFT es mejorar los mecanismos de consenso BFT iniciales. **PBFT es uno de los algoritmos de consenso más utilizados en redes blockchain permisionadas** ya que **requiere que los nodos estén identificados** y **se basa en la confianza previa entre los participantes** de la red ya que **todos persiguen un beneficio común**, sin embargo siempre **supone que existe información falsa circulando por la red** propagada por algunos nodos. **Existen dos tipos de nodos**: **los que pueden escribir información** en el blockchain **y el resto**; los que pueden escribir van rotando en secuencia (siguiendo un esquema *round robin*) de forma que en un momento dado le corresponde escribir un bloque a uno de ellos. Los nodos se encuentran ordenados en una secuencia concreta, de manera que además de verificar que la información proviene de un nodo concreto, también se verifica la validez de las transacciones.

En este algoritmo la **decisión se toma tras una votación en la que intervienen todos los nodos y suelen requerir un alto porcentaje de consenso (que al menos el 66% de los nodos validen las transacciones)**, lo cual supone que como máximo una tercera parte de la red pueda estar comprometida.

Se considera un algoritmo seguro y muy eficiente, y es utilizado entre otras por la plataforma Hyperledger.

### 2.8.6. Istanbul Bizantine Fault Tolerance – IBFT.

Es **la implementación más importante del algoritmo PBFT**. **Hay tres tipos de nodos**, los nodos que pueden **proponer transacciones**; los nodos **validadores que comprueban que los primeros tienen permiso para poder proponer transacciones, y los nodos que finalmente escriben** los bloques en la cadena con la información (transacciones) que proviene del resto de nodos.

Uno de las implementaciones donde se utiliza este algoritmo es ***Quorum***.

## 2.9. PROTOCOLOS

En muchos foros y ámbitos suele utilizarse la denominación protocolo a lo que acabamos de explicar anteriormente como algoritmo de consenso, encontrándose como sinónimas las expresiones "algoritmo de consenso" y "protocolo de consenso", pero **esta** identificación entre ambos términos en este contexto es incorrecta. Así, mientras que **los algoritmos de consenso** que hemos descrito se refieren a **una política** entre las partes **para alcanzar un acuerdo sobre lo que ha ocurrido y sobre quien escribirá el siguiente bloque**, los **protocolos** por su parte hacen referencia a la **tecnología concreta** que utiliza la red blockchain o a la implementación concreta en blockchain. Por ejemplo, Bitcoin y Ethereum son protocolos, mientras que PoW y PoS son los algoritmos de consenso que utilizan, respectivamente.

Los protocolos **hacen referencia al software** que se requiere en cada nodo **para comunicarse con los demás** en las redes blockchain, y **este software ha de ser el mismo en todos los nodos**. Del mismo modo que en Internet existe el protocolo TCP/IP o en el caso de envío de correos electrónicos existe el protocolo SMTP; en el caso de blockchain también hay estándares para que los nodos se comuniquen entre sí.

Así, **el protocolo es un concepto más amplio que el de algoritmo**, **ya que lo incluye como parte** del software necesario para que funcione la red al igual que incluye aspectos tales como el sistema criptográfico utilizado, el diseño de la cadena de bloques, las comunicaciones entre los nodos, las comprobaciones a realizar y el tipo de algoritmo de consenso utilizado.

A continuación destacamos algunos de los protocolos más relevantes.

### 2.9.1. Hyperledger

Proyecto iniciado en **2015** por la fundación **Linux**, de **código abierto**, y **orientado a redes privadas o permisionadas** con el objetivo de alcanzar estándares y protocolos en un marco universal, así como encontrar directrices para la implementación de redes blockchain en diversos ámbitos. El proyecto Hyperledger engloba **una gran cantidad de blockchain distintas** con **diversos algoritmos de consenso, reglas, modelos de identidad, tipos de almacenamiento, entre otros aspectos**, para utilizar blockchain en multitud de negocios, para lo cual ha desarrollado un **gran número de frameworks**, **librerías, interfaces gráficas, redes blockchain privadas, motores de smart contracts, etc.,** que pueden utilizar las empresas o los desarrolladores de forma modular lo que facilita la reutilización de componentes. Algunas de las herramientas que ofrece el ecosistema de Hyperledger para programar son Composer, Quilt, Cello, Caliper, Hyperledger explorer y Ursa.

Participan en el proyecto **más de 260 empresas** entre las que se encuentran varias multinacionales tecnológicas **como IBM, Intel, Cisco o SAP** así como del mundo de las finanzas como **BBVA**. **Cualquiera puede participar en este proyecto** mientras sea además miembro de **Linux Foundation**.

Existen **15 proyectos en Hyperledger[10], ninguno de los cuales trata sobre criptomonedas** ni tokens. Destacaremos los siguientes:

- Hyperledger **Besu**. Plataforma basada en Ethereum en casos de uso de **redes públicas y permisionadas** que incluye varios algoritmos de consenso tales como PoW y PoA.
- Hyperledger **Fabric**. Es una implementación modular para redes privadas en las cuales **sus miembros conocen las identidades y los roles de los otros miembros**; también implementa el concepto de **canales** en los que se despliegan casos de uso independientes. Pretende ser una solución versátil y modular para una amplia gama de diferentes casos de uso utilizando distintos algoritmos de consenso. En este protocolo se denomina *chaincode* a los smart contacts. Se trata de l**a implementación de Hyperledger más conocida**, siendo **IBM** uno de los contribuyentes principales.
- Hyperledger **Indy**. Es una plataforma es una plataforma con gran variedad de bibliotecas, herramientas y componentes reutilizables para ayudar a construir un sistema descentralizado basado en la **identidad en blockchain**, su principal contribución proviene del consorcio **Sovrin**.

[10] https://www.hyperledger.org

- Hyperledger **Iroha**. Orientado a proyectos relacionados con Internet of Things y al uso de dispositivos móviles, también incorpora la gestión de identidades. Programado en C ++ de forma modular.
- Hyperledger **Sawtooth**. Admite una gran variedad de algoritmos de consenso en una arquitectura modular orientada fundamentalmente a los *smart contracts,* en esta implementación los desarrolladores pueden definir las reglas de sus aplicaciones son necesidad de conocer el diseño del protocolo general y escribir sus *smart contracts* en una gran variedad de lenguajes de programación. INTEL es uno de sus principales desarrolladores.
- Hyperledger **Burrow**. Antes denominada ***Monax***. Ejecuta *smart contracts* siguiendo la especificación de Ethereum a través del lenguaje de programación *Solidity*.

### 2.9.2. Ethereum

Uno de los protocolos más extendidos es Ethereum, protocolo que apareció inicialmente de la mano del desarrollador **Vitalik Buterin** como una mejora del lenguaje de programación de bitcoin que permitiera realizar tareas más complejas. En la actualidad **es un lenguaje de programación de los denominados "turing completo"**, lo cual permite que se ejecute cualquier programa informático orientado a todo tipo de transacciones. En la actualidad se trata de una plataforma de código abierto orientada al desarrollo de ***smart contracts*** y dirigida a gran número de aplicaciones mucha de las cuales no tienen nada que ver con las criptomonedas.

En la red Ethereum se encuentra la criptomoneda *Ether*, la cual se utiliza del mismo modo que bitcoin, aunque también para para pagar capacidad de cómputo y de programación adquiriendo *gas*, un elemento propio de la red Ethereum que se utiliza para adquirir capacidad de cómputo, ancho de banda y almacenamiento.

### 2.9.3. Quorum

Otro proyecto de blockchain es Quorum, impulsado por **J.P. Morgan** para desarrollar **casos de uso de blockchain en el sector financiero**. Está **basado en Ethereum** y también se encuentra desarrollado bajo licencia de código abierto. Ahora **ya es posible utilizarlo en casos de uso que no estén relacionados estrictamente con el sector financiero**. Está **enfocado a redes privadas o permisionadas** donde los participantes se conocen entre sí al tiempo que se mantiene la privacidad de las transacciones.

### 2.9.4. Corda

R3 Corda es otro protocolo que está enfocado **al sector bancario**. Ha sido desarrollado por el consorcio de bancos **R3**, una start-up nacida en Nueva York que ha desarrollado este protocolo de código abierto denominado Corda en un principio orientado a la realización de transacciones entre los bancos sin necesidad de que haya una tercera institución vigilante. En la actualidad R3 **ya no es un consorcio de bancos, sino que se ha transformado en una empresa de software alrededor de la plataforma Corda** y se enfoca a más sectores además de la banca, como por ejemplo la cadena de suministro, el sector público, la energía, salud, telecomunicaciones, etc.

### 2.9.5. Multichain

MultiChain es un protocolo orientado a blockchain privadas, de manera que contiene un sistema de permisos para identificar quién puede operar en la red. No obstante permite cambiar el tipo de red y hacerla pública si se desea. También **es posible crear nuevas criptomonedas** en este protocolo y operar con ellas.

## 2.10. BLOCKCHAIN AS A SERVICE – BAAS

Existe un **modelo de negocio** en el cual empresas ofrecen plataformas de blockchain que permiten crear con facilidad aplicaciones y servicios digitales en una red distribuida a los clientes, mientras que **la empresa suministra la infraestructura y las herramientas de construcción** de la blockchain, así como garantizan ciertos aspectos relacionados con la seguridad. **La gran ventaja** de este modelo es que **no es necesario adquirir hardware ni software** siendo sencillo desplegar aplicaciones de registro distribuido sin necesidad de desarrolladores especializados.

Algunos ejemplos de estas empresas son IBM, especializada en Hyperledger Fabric; Microsoft ofreciendo servicios de R3 Corda, Hyperledger Fabric o Quorum, entre otras; Amazon; SAP; Oracle; Alibaba; Kaleido, etc.

## 2.11. MÁS ALLÁ DE LAS CRIPTOMONEDAS: OTRAS APLICACIONES DE BLOCKCHAIN

Blockchain y el ecosistema asociado de tecnologías de contabilidad distribuida se encuentra en una etapa temprana de desarrollo tecnológico, sin embargo al mismo

tiempo es una tecnología en rápida evolución y expansión que parece muy prometedora. El foco de aplicación de estas tecnologías se está desplazando desde el ámbito de las "criptomonedas" hacia nuevos lugares que requieren analizar las implicaciones políticas y legales de esta tecnología de manera más amplia al tiempo que se exploran las vías para dar una respuesta integral.

Ciertas propiedades derivadas de esta tecnología, tales como la inmutabilidad, la ausencia de terceras partes o la trazabilidad, entre otras, pueden ser muy útiles y encajar en determinadas soluciones.

A continuación señalamos **tan solo algunas** de las principales aplicaciones de blockchain que están surgiendo, cabe destacar que cada día aparecen nuevos proyectos en prácticamente todos los sectores de la industria.

### 2.11.1. Smart contracts

Una de las aplicaciones de las tecnologías blockchain, como hemos mencionado más arriba es el concepto de los denominados *smart contracts*. Se trata de programas informáticos cuyo código se encuentra escrito en los bloques de una cadena blockchain, por lo **tanto cada uno de los nodos posee una copia del mismo** y **no es posible modificar ese programa informático** (es inmutable). Además **puede ser ejecutado por todos los nodos y comprobarse (mediante un algoritmo de consenso) que el resultado obtenido es el mismo en todos ellos**, con lo cual se garantiza la transparencia y la seguridad del proceso al tiempo que se eliminan intermediarios. **Generalmente se trata de programas simples tipo *if… then*.**

Los contratos inteligentes se suelen utilizar para **automatizar tareas que habitualmente requieren de terceras partes de confianza** ya que en principio **pueden no necesitar de personas** que comprueben que un contrato se haya cumplido, esto es jueces o árbitros, de ahí la calificación de. En un contrato, que consiste en acuerdo entre partes, se especifican las condiciones o reglas en las que dicho contrato se ***smart*** ejecuta.

**A menudo será necesario que para comprobar el resultado de un contrato haya que acudir a una entidad externa a la red blockchain** para comprobar el cumplimiento de una clausula, a este tipo de entidad se le llama **oráculo** y ha de ser posible que el *smart contract* pueda conectarse a ese tipo de fuentes de información generalmente mediante APIs. Uno de los ejemplos más utilizados suele ser un *smart contract* que consulta una web que publica resultados deportivos para comprobar quien ha ganado una apuesta deportiva y transferirle las ganancias.

**Es posible interconectar diferentes *smart contracts*** entre sí aumentando la complejidad del sistema y dando lugar a lo que se conoce como **Organizaciones Autónomas Descentralizadas** (en inglés DAO), las cuales **son organizaciones completamente independientes y automatizadas en blockchain.**

### 2.11.2. Cadena de suministro. Trazabilidad.

En la industria de distribución y cadenas de suministro, los productos son digitalizados con un número de serie y son sometidos a un exhaustivo seguimiento. En este tipo de proyectos suele haber una **conexión estrecha entre blockchain y proyectos basados en *Internet of things* – IoT**, de forma que son los sensores quienes van escribiendo en el blockchain las condiciones del producto: posición, fechas, horas, condiciones físicas (humedad, temperatura, calidad del aire, etc), pagos de aduanas, tasas, calidad de materias primas, intervinientes, etc. De este modo es posible localizar cualquier producto al tiempo que se asegura que desde su producción hasta su entrega se han cumplido los estándares de calidad exigibles, siendo posible comprobar en blockchain todos los pasos por los que un producto ha transitado, dificultando la falsificación y facilitando la verificación y autenticación de la calidad del producto. Además es posible que intervengan todos los actores, empresas, proveedores, que intervienen en la creación de un producto desde el nivel más bajo hasta su entrega al cliente final.

En el caso de los sectores alimentario y agrícola se garantiza la seguridad de los alimentos en destino y cada vez son más los proyectos que utilizan blockchain en el sector de la agricultura donde, por ejemplo, muchas cooperativas pueden lograr que sus productos sean plenamente trazables e identificables y reducir así el riesgo de fraudes y falsificaciones.

### 2.11.3. Votación en blockchain

Las características de **transparencia, inmutabilidad y ausencia de terceras partes** en blockchain tienen aplicación también en sistemas de **voto electrónico** utilizando esta tecnología. Es posible diseñar sistemas de voto basados en blockchain que **impidan a una persona votar más de una vez**, **garantizar el secreto del voto**, **que no sea posible manipular los votos** emitidos, al tiempo que haya una gran facilidad para que **cualquiera consulte y haga contabilidad de los votos emitidos a las diferentes opciones**, lo cual

dota de una gran **trasparencia y seguridad** al proceso electoral y podría repercutir por ello en un **aumento de la participación** en los procesos electivos.

### 2.11.4. Sector financiero

Ya hemos explicado una de las aplicaciones más obvias para el sector financiero, el caso de las **criptomonedas**. Pero además, el sector bancario es uno de los más activos a la hora de utilizar blockchain en sus **procesos internos**. La mayoría de casos de uso en este sector utilizan esta tecnología en **proyectos donde participan varias entidades bancarias distintas** que han de relacionarse entre sí en el ámbito de procesos bancarios. También en proyectos que buscan **eliminar cierto tipo de intermediarios** que podrían ser sustituidos por una cadena de bloques. Se ha calculado que el uso de esta tecnología en el ámbito bancario le ahorraría a la banca sustanciales cantidades económicas al tiempo que aumentaría la eficiencia de sus procesos internos.

También han aparecido proyectos relacionados con microcréditos y la financiación participativa destinados a personas que no suelen tener acceso a financiación por los canales habituales.

### 2.11.5. Sector sanitario

Ha aparecido un gran número de posibles aplicaciones de la tecnología blockchain en el sector de la salud, tales como registrar el **libro de vacunas en blockchain**; o que el **historial médico** obre **en poder del ciudadano** y bajo su control; o que **la tarjeta de asistencia médica** se encuentre también en blockchain; también proyectos relacionados con el **control de medicamentos**; o datos sobre el **expediente de los médicos** que faciliten la burocracia que existe a la hora de trasladarse de destino.

### 2.11.6. Notariado de documentos

Es una de las aplicaciones más fáciles e inmediatas de uso de blockchain más allá de las criptomonedas. Consiste en **registrar un documento en blockchain** de manera que se

facilita su **verificación, su auditoría y su autenticación** al tiempo que hace imposible su manipulación.

### 2.11.7. Sector energético

Cada vez aparecen más proyectos en blockchain relacionados con la **trazabilidad del origen de la energía y** para **registrar el almacenamiento**, la **compra y venta** y **el uso** de la misma, así como para **certificar el origen de la energía**. También para automatizar mediante *smart contracts* ciertas tareas que se realizan manualmente. Estos proyectos **permiten la incorporación al mercado** junto a las grandes compañías energéticas de **pequeños productores individuales o cooperativas** que pueden producir y consumir ellos mismos su propia energía o venderla sin necesidad de intermediarios o terceras partes y con un alto grado de autonomía.

### 2.11.8. Aseguradoras

Blockchain tiene un alto potencial de uso en el sector de los seguros, en particular haciendo uso de los *smart contracts*, de manera que **automaticen procedimientos que hoy día requieren de la intermediación** y hagan que los procedimientos sean mucho más ágiles tanto para las aseguradoras como para los tomadores de seguros. También se asegura la transparencia respecto del objeto de los seguros y de las cláusulas de los mismos, ya que todo ello se encuentra en tecnología blockchain, registrando el alt**a de clientes, las pólizas y sus tarifas, la tramitación de los siniestros y la trasparencia en la consulta de información de las pólizas.**

## 2.12. APLICACIONES DE BLOCKCHAIN EN LAS ADMINISTRACIONES PÚBLICAS

### 2.12.1. European Blockchain Partnership

La Comisión Europea está apostando decididamente por la tecnología blockchain con el ánimo de que la Unión Europea se convierta en líder mundial en esta tecnología.

En octubre de 2017, el Consejo de Europa solicitó a la Comisión Europea que adoptara medidas en relación a blockchain con iniciativas para mejorar las condiciones que permitan que la Unión Europea explore nuevos mercados y consiga posicionarse como líder en los mismos.

A continuación, en febrero de 2018 la Comisión Europea puso en marcha el Observatorio y Foro Europeo de Blockchain (*EU Blockchain Observatory and Forum*[11]) con el ánimo de acelerar la innovación y el ecosistema de desarrollo en blockchain dentro de la Unión Europea. Se trata de un foro para compartir conocimiento, identificar obstáculos y encontrar soluciones para el establecimiento de esta tecnología. También anunció que invertiría unos 300 millones de euros en proyectos para apoyar el uso de blockchain a través de su programa de investigación e innovación Horizonte 2020.

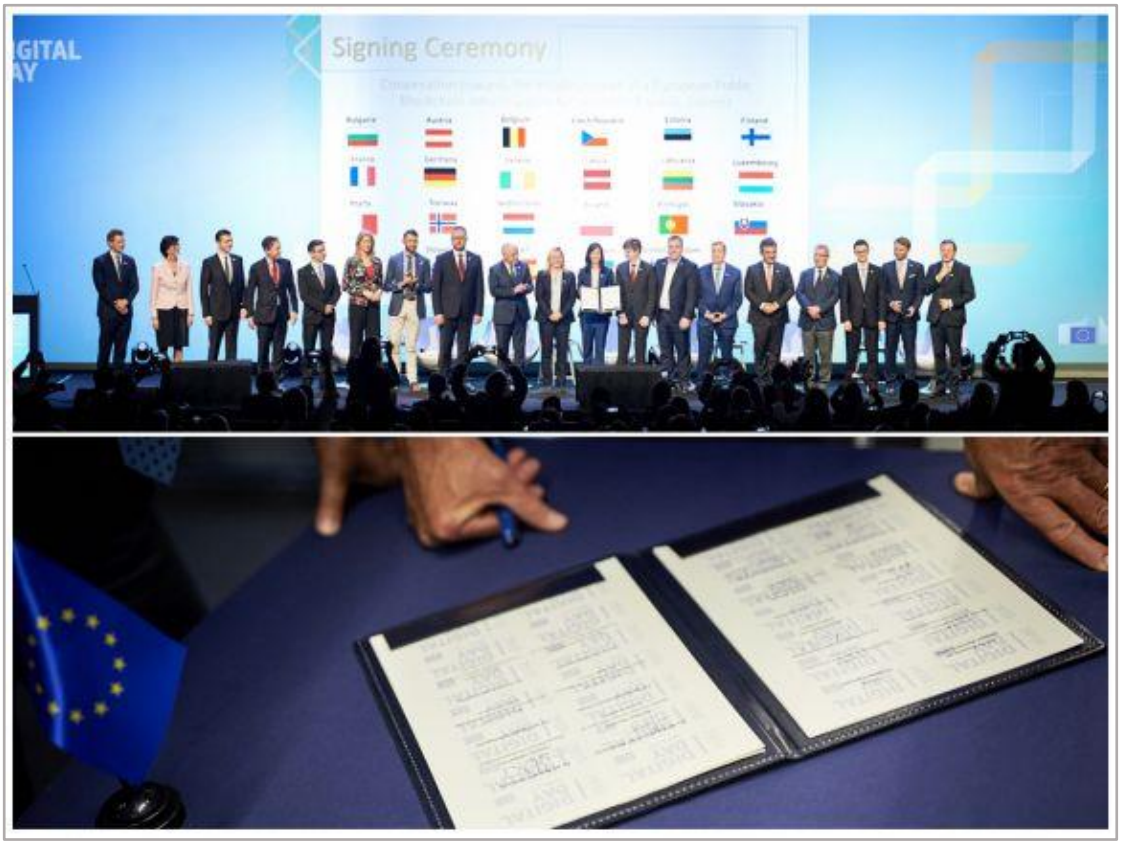



*Ilustración 4. Firma del European Blockchain Partnership el 10 de abril de 2018.*

[11] https://www.eublockchainforum.eu/

El 10 de Abril de 2018, durante la celebración del *Digital Day* en Bruselas, 22 países europeos, incluyendo a España, firmaron la Declaración de Cooperación para establecer una asociación europea de Blockchain[12]. El principal objetivo de este *European Blockchain Partnership* (EBP), que reconoce el compromiso de estos países con el potencial de esta tecnología para transformar los servicios digitales tanto en el sector público como en el privado, es la creación de una red europea de servicios basados en blockchain (*European Blockchain Services Infrastructure – EBSI*). A continuación, se propuso un calendario que contemplaba tener cerrada la definición de las especificaciones técnicas y el modelo de gobernanza de esa red para finales de 2018 y lanzar los primeros servicios transfronterizos hacia finales de 2019. En la actualidad el número de países firmantes de esa declaración asciende a 30: todos los países de la UE más Noruega y Liechtenstein.

Algunas de las características que se persiguen en esa red de blockchain europea EBSI son las siguientes:

- Ha de ser una red de tipo pública y permisionada, por tanto ha de ser conocida la identidad de todos los nodos participantes, los cuales entran a forman parte de la red tras serles aceptada su solicitud de participación en un proceso definido.
- La red ha de ser escalable de manera que permita un alto número de transacciones (*throughput*) y de nodos.
- Ha de ser una red abierta utilizando sistemas *open-source.*
- EBSI debe ser sostenible marcándose altos objetivos de eficiencia energética.
- Ha de ser una red interoperable que se base en estándares y especificaciones técnicas reconocidos.

En el año 2018 concluyó el debate entre los países firmantes sobre la selección de los primeros casos de uso específicos a implementar en la EBSI, así como se definieron un modelo de gobernanza y los principios rectores del modelo. En esta primera fase de la red, los criterios de selección de nuevos casos de uso han sido los siguientes:

- **Servicios / procesos del sector público**: el caso de uso debe basarse en una necesidad claramente identificada de las autoridades públicas y el servicio o proceso debe estar claramente identificado dentro de la competencia pública.
- **Dimensión transfronteriza**: el caso de uso debe referirse a procesos o servicios que involucran transacciones u operaciones que involucran a varias administraciones de los Estados Miembros.
- **La tecnología blockchain debe agregar de forma clara valor añadido a la solución**. El caso de uso debe estar respaldado por indicadores suficientes de que

[12] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51818

la tecnología blockchain aumenta la eficiencia, la mejora, apoyando las políticas de la UE y las estrategias industriales, etc.

Los primeros tres casos de uso elegidos para implementar en la red EBSI han sido: *European Self-Sovereign Identity Framework – ESSIF* (traducido como identidad digital soberana o autogestionada), *Diplomas Académicos* y por último *Notarización* de documentos. Los tres casos de uso se describen más adelante en este documento.

En 2019 comenzaron los trabajos de construcción de la plataforma EBSI así como el desarrollo de los tres casos de uso seleccionados. Para ello, la Comisión Europea en conjunto con los países firmantes del EBP ha creado cinco grupos de trabajo, tres de ellos correspondientes a cada uno de los tres casos de uso elegidos y dos grupos de trabajo más, los grupos "Policy" y "Technical". El grupo "Policy" se orienta a la gobernanza general del proyecto, al estudio de aspectos legales, de estandarización o la selección de nuevos de casos de uso a implementar en la plataforma entre otros aspectos; el grupo "Technical" tiene la función de definir los requisitos técnicos de la red de manera que dé cabida a los casos de uso elegidos y sea lo suficientemente flexible como para acoger otros casos de uso en el futuro; en el resto de casos de uso se trabaja para definir el modelo de información correspondiente a cada caso de uso elegido. En cada grupo de trabajo participan representantes designados por los respectivos países.

España participa en cuatro de esos grupos de trabajo, a saber, los grupos "Policy", "Technical", "ESSIF" y "Diploma" y ha designado representantes en esos grupos de trabajo. La Secretaría General de Administración Digital coordina todos esos grupos mediante reuniones periódicas de un grupo de trabajo interno denominado GT-Blockchain.

En estos momentos (febrero de 2020), la Comisión Europea ha desplegado varios nodos de la red EBSI bajo su control, y ha distribuido entre los países miembros del EBP un "kit de despliegue" que permite que en cada uno de estos países se despliegue uno o varios nodos de esa red para comenzar las pruebas de los casos de uso que se han implementado. En este momento se encuentran ya operando 27 nodos de 15 países.

Para la Comisión Europea, el éxito de esta apuesta en blockchain se sostiene en cinco grandes pilares, a saber:

- La estrecha colaboración entre los países miembros del **European Blockchain Partnership** para desarrollar la red EBSI con servicios públicos transfronterizos.
- Impulsando la **creación de un consorcio** formado por todos aquellos interesados (fundamentalmente del sector privado tales como empresas, instituciones, etc.). Este consorcio se denomina **INATBA** (International Association of Trusted Blockchain Applications). La Comisión Europea considera clave la colaboración

público-privada para lograr el objetivo de que Europa sea una referencia en esta tecnología y considera que para ello es necesario que se produzca un diálogo fluido entre el sector privado y las instituciones públicas que permita definir el futuro marco regulatorio de las tecnologías de registro distribuido de forma que surja una convergencia que evite la aparición de enfoques fragmentados.

- Mediante la **creación del Observatorio y Foro Europeo de Blockchain** que permite aglutinar conocimiento en esta materia y realizar recomendaciones, estudios, análisis y ofrecer soluciones a posibles problemas que puedan aparecer.
- **Invirtiendo en investigación e innovación** a través de los programas Horizonte 2020 y *Connecting Europe Facility* (CEF).
- **Promoviendo un entorno legal y regulatorio**, con estándares interoperables e impulsando el desarrollo de habilidades en blockchain.


*Ilustración 5. Acciones promovidas desde la Comisión Europea para impulsar blockchain en la UE.*

El 14 de febrero de 2019 la Comisión Europea publica el programa de trabajo de telecomunicaciones para el año 2019 de *Connecting Europe Facilities* (CEF), una herramienta de financiación de proyectos para promover crecimiento económico, empleo, competitividad e inversiones en el seno de la Unión Europea que ya crea las condiciones de financiación de la plataforma EBSI.

#### 2.12.1.1 El caso de uso ESSIF – Identidad Autogestionada

Como se ha comentado más arriba, a blockchain se le atribuye haber creado el internet del valor, ya que permite transferir valor entre distintas entidades sin necesidad de que haya terceras partes, esto produce la necesidad de solucionar uno de los grandes problemas de internet: el **problema de la identidad, dado que en muchos contextos es necesario saber sin género de dudas quiénes son los intervinientes en una transacción, o quién está detrás de un activo**, y aquí blockchain también se puede utilizar para resolver este problema.

**Internet** desde sus inicios **se pensó para interconectar máquinas**, **para transferir y almacenar información**, pero generalmente es **difícil saber quién se encuentra al otro lado de la conexión de internet.** En el año 1993 se publicaba el famoso chiste del perro en Internet (no se sabe si quien está conectado en Internet es un perro) que muestra cómo ya entonces existía conciencia de este problema. Hoy día el problema sigue sin solucionarse, además, toda la información sobre la identidad consiste en el rastro de información que los usuarios van dejando en los sitios web de terceros, esto es, la información está almacenada y controlada por esas terceras partes que controlan los sistemas de almacenamiento en que se encuentra nuestra información personal (Google, Facebook, Amazon, Linkedin, bancos, aseguradoras, empresas de servicios, administraciones públicas, etc.).


*Ilustración 6. Chiste aparecido en 1993 en el periódico The New Yorker*

Cuando un usuario se registra en cualquier servicio, como Netflix, Spotify, Facebook, Twitter,… (por mencionar sólo algunos de los más populares), proporciona algunos datos personales (típicamente nombre, edad, sexo, correo, teléfono, contraseñas, tarjeta de crédito, etc.) que a partir de entonces **se encuentran bajo el control de la organización que nos proporciona el servicio** al conectarnos utilizando los identificadores digitales más comunes, como puedan ser las direcciones de correo electrónico o los nombres de usuario y contraseñas.

Esas terceras partes, también denominadas **silos de información,** pueden además **comerciar con nuestros datos, utilizarlos en su beneficio, realizar perfiles de todo tipo**,… también son quienes custodian esos datos, de forma que si sus sistemas caen o se corrompen los datos se ven afectados. Por tanto, en este modelo existen **problemas de seguridad y problemas en relación a la privacidad de los datos personales**.

**Ha habido varios modelos de identidad** desde los inicios de Internet, en donde cabe destacar tres: **la identidad centralizada basada en usuario y contraseña**; **la identidad federada y compartida entre varias compañías** (por ejemplo el modelo de Liberty Alliance o el primer Microsoft's Passport); o **la identidad dependiente de proveedores de identidad** (caso de Open ID, Facebook, Google, Linkedin,…). **En todos los casos siempre hay un tercero en quien se confía que custodia los datos de identidad**, por ese motivo siempre se han producido esfuerzos en diseñar sistemas en donde la identidad estuviera bajo el control de su dueño.

En el año **2005**, **Kim Cameron**, experto en tecnologías de identidad, publica el artículo ***Las leyes de la identidad***[13], artículo que comienza indicando esta misma idea: "*Internet fue construida sin una manera de saber quién y a qué te estas conectando. Esto limita lo que podemos hacer y nos expone a peligros crecientes. Si no hacemos nada enfrentaremos rápidamente una proliferación de episodios de robo y fraudes que acumulativamente erosionarán la confianza pública en Internet*". **Las ideas y siete principios de la identidad de ese artículo han influido en los paradigmas europeos de protección de datos personales que han confluido en el GDPR (*General Data Protection Regulation (EU) 2016/679*),** tales como el consentimiento del usuario que establece que los datos han de encontrarse bajo control de su dueño y sometidos a su consentimiento, a que los datos que se proporcionen han de ser lo mínimos necesarios para el fin que se solicitan, esto es, han de estar justificados.

**Uno de los conceptos más novedosos en el área de blockchain es el denominado "Identidad digital autogestionada" (*Self-Sovereign Identity* en inglés)** referido a un tipo de identidad digital donde el usuario es el propietario de sus datos y tiene pleno control sobre ellos. De esta manera, el usuario decide qué datos comparte con qué terceros y en qué términos. **Dado que se trata de una idea emergente existe una gran confusión en muchos ámbitos en torno a lo que significa este concepto.** Esta **confusión** se **deriva** fundamentalmente **de confundir identidad con identificación.** Así que, de entrada hay que aclarar que mientras que la identificación es solamente uno de los datos personales que nos pertenecen (el número del DNI por ejemplo en el caso de España), la identidad consiste en la suma de todos los datos personales que nos incumben (incluyendo el DNI en nuestro ejemplo), tales como la altura, la edad, sexo, titulaciones académicas, libro de familia, carné de estudiante, carné de conducir, títulos de propiedad, etc... Podría decirse que es la suma de lo que somos, lo que podemos hacer, lo que tenemos, lo que dicen de nosotros,… en definitiva cualquier atributo que se pueda predicar sobre una persona o

[13] https://www.identityblog.com/?p=352

entidad, ya que bajo el ámbito de la identidad autogestionada, el usuario puede ser una persona física, jurídica, o un objeto.

Lo novedoso de esta tecnología consiste en que **el usuario tiene el control sobre sus datos** personales porque los custodia él mismo y no un tercero, decidiendo quién tiene acceso a esos datos y en qué condiciones, de ahí el término "*sovereign*" en inglés, indicando que es el usuario el dueño y soberano de su información, y no otros. Así, no es necesario acudir a una tercera parte que atestigüe lo que afirmamos sobre nosotros mismos. Por tanto, un proyecto de identidad digital autogestionada consiste en que es el usuario quien guarda sus datos personales en su teléfono móvil, en la nube o en cualquier dispositivo bajo su control. Datos digitales como por ejemplo, el DNI, el carné de conducir, títulos académicos, registros de la propiedad, libro de familia, etc. y es el propio usuario quien decide a quien dar esos datos y para un propósito concreto. **Por supuesto los emisores de esos datos siguen siendo los mismos que ahora**: la Policía Nacional, las universidades, la Dirección General de Tráfico, los registros, etc., esto es, la fuente de la validez de la información permanece en los orígenes actuales o fuentes primarias de datos, pero una vez emitidos los datos ya permanecen bajo el control de su destinatario sin que este emisor conozca el uso que se está haciendo de los mismos, esto es, el emisor de la información no conoce que la información que ha emitido pueda ser verificada por otro, porque ya no es necesario acudir a él para hacerlo. Con este sistema además, no es posible relacionar los múltiples datos vinculados a una persona o entidad.

Este tipo de proyectos se encuentra en una fase muy inicial, además se enfrentan a problemas de interoperabilidad de la información, de ausencia de estándares y de tecnologías claras que ya se encuentren funcionando. También son muy dependientes de la información que se pretenda utilizar o del caso de uso concreto (diplomas académicos, permiso de conducir, etc).

**La identidad autogestionada es**, **según** el experto en la materia, **Christopher Allen** (y uno de los fundadores de SSL – *Secure Sockets Layer*), **la cuarta fase en la evolución de la identidad digital,** tal y como lo explica en 2016 en su artículo ***The Path to Self-Sovereign Identity***[14]. A él se le atribuye el haber acuñado el término de *Self-Sovereing Identity* y muchos de los proyectos en marcha se guían por los 10 principios que Allen formula en su texto. **Varios de ellos los hereda de Cameron**, pero cabe destacar el primero, por novedoso y porque explica uno de los principios más fuertes de este tipo de identidad: el principio de *existencia*. Con este principio, Allen pone a **la identidad digital al mismo nivel que la identidad en el mundo real**, **existe por sí misma**, sin necesidad de apoyarse en terceros que refrenden la información sobre nosotros. Los diez principios de Allen de la identidad autogestionada son los siguientes:

- **Existencia**. Los usuarios tienen una existencia digital independiente, autónoma y por sí misma.

[14] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

- **Control**. Los usuarios tienen el control sobre su propia identidad y es la máxima autoridad sobre la información que se refiere a él mismo. Siempre deben ser capaces de referirse a ella, actualizarla o incluso ocultarla.
- **Acceso**. Los usuarios deben tener acceso a sus propios datos. Un usuario siempre debe ser capaz de recuperar fácilmente la información sobre su identidad. Sin barreras y sin intermediarios.
- **Transparencia**. Los sistemas y algoritmos para administrar y operar una red de identidades deben ser abiertos y transparentes tanto en su funcionamiento como en la forma en que se gestionan y actualizan. Cualquier persona debe ser capaz de examinar cómo funcionan.
- **Persistencia**. La información sobre las identidades deben durar al menos durante el tiempo que el usuario desee. Esto ha de ser compatible con el "derecho al olvido", de forma que un usuario debe poder modificar o eliminar datos sobre su identidad.
- **Portabilidad**. El usuario debe poder transportar consigo mismo sus datos de identidad sin que esos datos se encuentren en poder de terceras partes. Debe ser posible transportar y utilizar los datos personales en cualquier punto del globo sin tener en cuenta fronteras físicas.
- **Interoperabilidad**. Los datos de identidad deben poder ser ampliamente utilizables sin estar restringidos a funcionar en sistemas informáticos concretos.
- **Consentimiento**. Los usuarios deben estar de acuerdo en el uso que se hace de los datos sobre su identidad.
- **Minimización**. El número de datos personales que se proporcione a un tercero debe ser el mínimo necesario justificado para alcanzar el fin que se persigue.
- **Protección**. Han de protegerse los derechos de los usuarios. En caso de conflicto entre los intereses de la red y los de los usuarios individuales la balanza se inclinará en el sentido de la preservación de las libertades y derechos de las personas

**El caso de uso que se ha puesto en marcha en la red EBSI es un proyecto de identidad autogestionada que, en combinación con el sistema eIDAS, es el proyecto que sustenta todos los demás casos de uso sobre los que se está trabajando en el proyecto europeo, dado que cualquier caso de uso no deja de ser un atributo de nuestra identidad (algo que somos, algo que tenemos, etc.).**

Veamos el modelo de funcionamiento del caso de uso de identidad autogestionada que se ha puesto en marcha en la red EBSI. Como hemos visto en el caso de bitcoin, el usuario puede demostrar que él es quien controla una dirección de blockchain (y sus bitcoin asociados) porque es quien posee la clave privada asociada a la clave pública que se encuentra en esa dirección, y no olvidemos que esa clave pública se encuentra replicada en todos los nodos participantes en la red. Este es uno de los motivos por los que en blockchain el tipo de criptografía utilizada es la de curva elíptica, dado que es un

sistema muy seguro, su generación de claves tiene un menor coste computacional y es posible generar infinitas claves públicas.

**En el ámbito de la identidad autogestionada, a esa dirección de blockchain se le denomina Identificador Descentralizado – DID (*Decentralized Identifier*[15]).** De forma simplificada un DID no es más que **un par de claves criptográficas pública / privada** junto con un **código alfanumérico consistente en una dirección URL que apunta al lugar de una blockchain concreta en donde se encuentra la clave pública**, lo cual **permite demostrar que toda la información que se asocie a esa dirección blockchain se encuentra controlada por quien posee la clave privada almacenada en su *wallet***. Se trata un estándar abierto del consorcio W3C que puede funcionar en cualquier blockchain pública o privada.


*Ilustración 7. Esquema de un DID en la EBSI*

Es importante destacar que **un DID no contiene datos personales**, y que **es posible que un usuario posea múltiples DID. Una vez obtenido un DID, es posible vincular al mismo un conjunto de credenciales (*Verifiable credentials*[16]) que se almacenan en el *wallet* del usuario y son controladas por el mismo. Las credenciales son información (atributos, afirmaciones) sobre un usuario que son firmadas digitalmente por quien puede realizar esas afirmaciones sobre el usuario en cuestión y vienen a decir que el usuario A, quien posee un $DID_A$ (lo que permite localizar la clave pública de A en un blockchain) firma con su clave privada y localizada en su *wallet* una credencial (en EBSI es un documento en formato JSON) en el que dice algo sobre el poseedor del $DID_B$.** Probablemente, para que $DID_A$ afirme algo sobre $DID_B$, habrá sido necesario que B se identifique ante A,

[15] https://www.w3.org/TR/did-core/
[16] https://www.w3.org/TR/vc-data-model/

aunque esto no siempre será imprescindible (es posible realizar afirmaciones sobre alguien sin conocer su identidad). Por este motivo las credenciales tienen niveles de confianza, en función de la fortaleza que haya tenido la identificación.

Todos los actores que participan en este modelo tienen sus propios DID, lo cual posibilita que cualquiera pueda actuar bien como emisor o bien como receptor de credenciales. En caso de actuar como emisores de credenciales, es posible que a su vez otra entidad tenga que atestiguar que efectivamente somos una autoridad competente para emitir ese tipo de credenciales verificables, y así sucesivamente hasta llegar a lo que se conoce como anclas de confianza (*anchor trust*) o raíz del árbol de información.

**Una red de blockchain permite que sea posible verificar que las credenciales han sido firmadas por sus emisores sin necesidad de consultarles a ellos, por tanto éstos no podrán conocer el uso que se está haciendo de las credenciales que han emitido**, encontrándose la información personal bajo el control de su dueño. Además, si los nodos de esa red se encuentran distribuidos por todo el planeta, ningún país, institución o individuo pueden controlar la información sobre las credenciales que posee un usuario en su wallet. En una red de blockchain como la EBSI podrá comprobarse incluso desde más allá de las fronteras de la UE que una credencial es auténtica, esto es, que ha sido emitida por quien tiene autoridad para hacerlo y pertenece al usuario que la presenta. Ya se están planteando proyectos transfronterizos para que los **refugiados** que huyen de sus países puedan obtener una identidad de este tipo que trasciende las fronteras; la ONU ya ha recomendado explorar esta posibilidad[17] así como han aparecido iniciativas en este sentido en Europa[18], tales como las iniciativas MONI de Finlandia o Taqanu[19].

A continuación en la siguiente tabla se muestran algunos ejemplos de las credenciales que un usuario X, en poder del $DID_x$ tiene en su wallet. Nótese que en el último caso de la tabla, es el propio usuario X quien ha emitido una credencial a otro usuario Y.

[17] https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B
[18] https://www.acnur.org/5d27b4814.pdf
[19] https://www.taqanu.com/

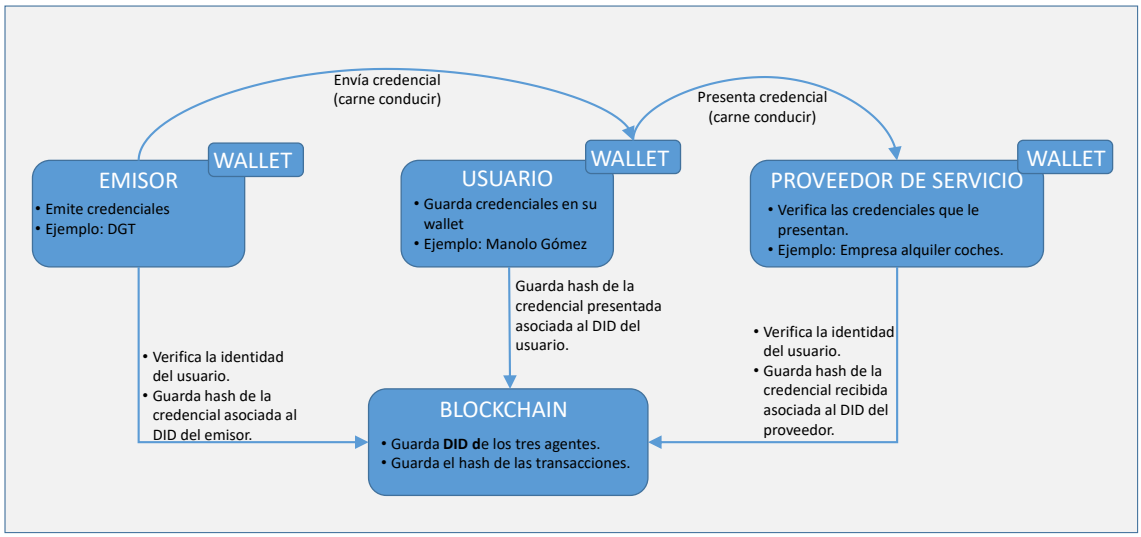
| Emisor de la credencial | Información contenida en la credencial |
|---|---|
| Policía Nacional ($DID_{PN}$) | El poseedor del $DID_x$ tiene asociados los datos que constan en el DNI (nº de DNI, nombre, apellidos, fecha de nacimiento, nombre de sus padres, dirección, fecha y equipo de expedición, etc. |
| Dirección General de Tráfico ($DID_{DGT}$) | El poseedor del $DID_x$ posee un carné de conducir tipo B1, fecha de expedición, fecha de validez, etc. |
| Ministerio de Ciencia, Innovación y Universidades ($DID_{MICIU}$) | El poseedor del $DID_x$ posee un título de licenciado en Derecho por la Universidad Autónoma de Madrid, fecha de expedición, etc. |
| Registro Civil ($DID_{RC}$) | El poseedor del $DID_x$ es padre de María, nacida el día, etc. |
| Banco de Santander ($DID_{BS}$) | El poseedor del $DID_x$ es titular de una cuenta bancaria Nº xxxxxxxxxx |
| Banco Bilbao Vizcaya ($DID_{BBVA}$) | El poseedor del $DID_x$ es titular de la tarjeta xxxx.xxxx…. con fecha de validez 1/06/2023 |
| YouTube ($DID_{YT}$) | El poseedor del $DID_x$ tiene un video en YouTube (https:/www.youtube.com…) que a fecha XX/XX/XXXX ha recibido 58.735 visitas. |
| Alberto García ($DID_{AG}$) | El poseedor del $DID_x$ es mi amigo. |
| Soluciones Integradas e Integrales SL | El poseedor del $DID_x$ ha trabajado en esta empresa desde 20/04/2007 hasta 15/07/2019 |
| Agrupación museros asturianos | El poseedor del $DID_x$ ha vencido en el torneo de mus de Gijón el 12/02/2018 |
| Universidad Complutense de Madrid ($DID_{UCM}$) | El poseedor del $DID_x$ está matriculado en esta universidad en el grado XXXX. |
| Vodafone ($DID_{VOD}$) | El poseedor del $DID_x$ es titular de la línea 675 56 87 77. |
| Registro de la propiedad ($DID_{RP}$) | El poseedor del $DID_x$ es dueño de una finca situada en…, etc. |
| Ayuntamiento de Madrid ($DID_{AM}$) | El poseedor del $DID_x$ está empadronado en Madrid, calle, número, etc. |
| Agencia Tributaria ($DID_{AEAT}$) | El poseedor del $DID_x$ se encuentra al corriente en sus obligaciones tributarias estatales. |
| Todo Tatoo ($DID_{TTOO}$) | El poseedor del $DID_x$ se ha realizado en este establecimiento un tatuaje de características: …, lugar del cuerpo:…, etc. |
| Josefina López ($DID_{JL}$) | El poseedor del $DID_x$ me parece muy simpático, agradable e inteligente. |
| Gimnasio BestFit ($DID_{BF}$) | El poseedor del $DID_x$ puede entrar en este gimnasio. |
| Poseedor de $DID_x$ | El poseedor del $DID_y$ ha sido trabajador del hogar en mi casa durante dos años y quiero destacar que es una persona limpia, ordenada y eficiente. |

*Ilustración 8. Ejemplos de credenciales que el usuario X posee en su wallet.*

Como se puede apreciar en la tabla anterior, aunque la estructura general de una credencial es siempre la misma, pueden variar los metadatos asociados al cuerpo de la información que se incluyen (puede ser tan solo "mide 190 cm" o un conjunto de muchos más: DNI + Nombre + Apellidos + Dirección + etc.). También hay que destacar que ahora el sujeto de todos los atributos de identidad pasa a ser el DID.

En el modelo de identidad que se está desarrollando en la EBSI las credenciales no se almacenan en la red de blockchain, sino que se encuentran en poder de los propios usuarios en sus wallet, por lo que estos datos se dice que se encuentran *offchain*. La información que se almacena en blockchain es el registro de transacciones que se produce entre los usuarios. Estas transacciones son fundamentalmente las peticiones que se hacen a un usuario para que proporcione una información a alguien para un propósito específico, por ejemplo la empresa Hertz solicita Manolo Gómez su permiso de circulación para alquilarle un coche, pues bien, el *hash* de esta petición con una estructura y formato específicos en JSON es lo que se almacena en blockchain, combinando información en ese archivo en JSON del emisor y del receptor de la información.

El esquema que explica las transacciones es el siguiente:




Vemos que dado que en la red blockchain se almacenan los hashes que se han generado a partir de la combinación entre credenciales y los DID de los diferentes actores, no es posible relacionar información entre emisores y proveedores de servicio, además tampoco es posible crear perfiles de usuario a partir de los hashes que va guardando en la cadena de bloques, dado que estos no se repiten. Además en blockchain no se almacena información de carácter personal, la cual permanece siempre en el *wallet* del usuario. Con esta implementación se busca que la red EBSI sea lo que se denomina "*GDPR compliant*" de forma que sea compatible con lo estipulado en el Reglamento General de Protección de Datos. Ni siquiera sería posible averiguar la actividad de grandes empresas como por ejemplo Movistar, ya que por ejemplo, el hipotético alta en este modelo de blockchain de los cerca de 20 millones de clientes de telefonía móvil de Movistar supondría 20 millones de *hashes* diferentes, puesto que cada *hash* se ha calculado a partir de una semilla construida con información de Movistar y con información del cliente.

Aunque en blockchain no se puede alterar la información referente a una credencial, sí que se puede escribir que esa credencial está revocada, esto es, el emisor (la DGT en nuestro ejemplo del esquema), podría escribir que el permiso de circulación de Manolo Gómez está revocado porque se le ha retirado (o que ya no es cliente de Movistar).

Por supuesto es inevitable que los proveedores de servicio tengan datos personales de sus clientes, pero al almacenar en blockchain transacciones que se refieren a que se ha dado el consentimiento para un propósito determinado, junto a la posibilidad de revocar ese consentimiento, le da al ciudadano el control de sus datos. Los proveedores de servicio continuarán teniendo una copia de los datos personales pero no podrán usarlos más que para el fin para el que su dueño les haya autorizado, en caso contrario será posible demostrar en un blockchain que esos datos han sido utilizados para una finalidad distinta.

No obstante nadie, excepto el propio usuario, puede suspender ni revocar el DID.

En otro tipo de implementaciones menos seguras que la que se emplea en la EBSI, se podría, mediante ingeniería de datos, descubrir la identidad de los usuarios incluso aunque en blockchain sólo se almacenaran hashes o pseudónimos de los usuarios. El análisis de la actividad de esos hashes o pseudónimos permitiría realizar perfiles de comportamiento de usuarios e incluso, llegado el caso, identificarlos.

**Ventajas para el ciudadano**

- **Control de la información.** La información la porta el ciudadano en su monedero y ya no es necesario remitir al proveedor original de la información para demostrar que es válida. Basta con remitir a una red de blockchain. Blockchain se convierte en el "intermediario" de las actuales transacciones con los proveedores de información. Es posible entregar una credencial a un receptor y posteriormente revocar la capacidad de uso de esa credencial a ese receptor.
- **Privacidad.** Todo está cifrado mediante claves criptográficas (clave pública/privada). La información en cualquier transacción sólo es visible para los participantes de la misma. **También se guarda el propósito** de la transacción de manera que el receptor de la información personal sólo la utilice para el fin que la pidió y durante el tiempo necesario, lo cual proporciona al dueño de la información la protección de su información y, de nuevo, su control.
- **Seguridad.** La información se encuentra distribuida en múltiples nodos de blockchain, lo que complica considerablemente la alteración o manipulación de la información. En este punto, la seguridad es la que aporta la propia tecnología blockchain.

Hay varias implementaciones de sistemas de identidad autogestionada además del desarrollado en la red EBSI, tales como los de Sovrin, u-Port, Evernym, Microsoft ION o la del consorcio Alastria en España. Además, la comunidad de desarrolladores trabajando en este tipo de modelos es muy amplia destacando los siguientes grupos por su grado de avance y consenso en las materias que tratan:

- **W3C**. Este consorcio **ha definido el DID**, en la capa más baja de la blockchain. Como se ha señalado se trata de un identificador que el propio usuario genera y que se corresponde a una dirección única en blockchain, siendo posible que el mismo usuario obtenga tantos DID como desee para, posteriormente, asociar a cada uno de ellos la información que considere oportuna.

  **También** desde W3C se trabaja en la capa correspondiente a **las credenciales verificables,** las afirmaciones que terceras partes realizan sobre los usuarios y que los mismos almacenan en sus *wallet* en forma de atributos de su identidad para poder presentarlos a su vez con otras terceras partes.

Otro área relevante en el que se trabaja desde este consorcio es en los conocidos como **modelos ZKP (*Zero Knowledge Proof*), o prueba de conocimiento cero,** un área emergente y muy prometedora que se basa en la idea de **que la mejor forma de proteger la información es no entregarla nunca.** Es posible demostrar que se poseen ciertos atributos de identidad sin revelar información sensible, el caso típico es del de demostrar que se es mayor de edad sin revelar la fecha de nacimiento o sin decir la edad propiamente, por ejemplo en una página web de venta de bebidas alcoholicas online que exija demostrar que el comprador es mayor de edad o en la entrada a una sala de fiestas que también exija ser mayor de una edad concreta. Se trata de **algoritmos criptográficos que dada una credencial verificable con una cierta información permiten generar pruebas hacia terceros de que se cumple una condición de identidad sin revelar el contenido de la credencial, garantizando de este modo altos niveles de privacidad.**

- **OASIS**. Se centra en la **gestión de claves** en sistemas denominados **DKMS (*Decentralized Key Management Systems*)[20].** Como hemos visto hasta ahora, la criptografía desempeña un papel fundamental en blockchain, por lo que también se hereda uno de los problemas que siempre han estado asociados a estos sistemas, la gestión de claves criptográficas y a estudiar mecanismos que permitan acceder a la información en caso de perder el acceso a nuestro wallet. En este campo se está trabajando fundamentalmente **en dos tipos de mecanismos**, el denominado **"*paper wallet*"** consistente en memorizar una serie de doce palabras que nos permitirían recuperar nuestros datos; y el **denominado "*social recovery*"** basado en la confianza que se deposita en un conjunto de personas que pueden atestiguar llegado el caso que efectivamente somos quienes decimos ser y en quien podemos repartir la información.

- **DIF** (*Decentraliced Identity Foundation*). Está trabajando en la **capa de autenticación** estudiando la **compatibilidad de estos sistemas de identificación autogestionada con modelos tradicionales no blockchain** que tendrán que convivir con este nuevo tipo de formas de identificación. Ya se ha definido un conjunto de varios modelos diferentes de autenticación que dependen del caso de uso concreto, del tipo de dispositivo, etc.

Finalmente cabe señalar que se espera que existan un gran número de redes blockchain separadas, dado que es imposible que exista una sola para todos los casos de uso, no obstante será posible interconectarlas entre sí una vez haya estándares aceptados asentados que permitan la interoperabilidad de las diferentes redes entre sí.

[20] https://github.com/hyperledger/indy-sdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md

#### 2.12.1.2 El caso de uso de "Diplomas"

**El resto de casos de uso en la EBSI son una extensión del de la identidad autogestionada, dado que todos ellos consisten esencialmente en definir el contenido de las credenciales que les atañen.** Por ese motivo es necesario que se constituyan **grupos de trabajo** formados por representantes de los Países Miembros expertos en el caso de uso que se trate. En el caso concreto de "Diplomas" los representantes de cada país provienen típicamente de administraciones públicas relacionadas con el mundo universitario y los títulos académicos.

El caso de uso de Diplomas consiste en que cuando un estudiante europeo acaba un grado universitario o cualquier titulación oficial reconocida, ese diploma o título universitario se expide por parte de la institución autorizada en cada país en forma de credencial verificable para que el estudiante la guarde en su *wallet* de la red EBSI. Esto permite solucionar varios problemas que enfrentan los ciudadanos hoy día cuando tratan de hacer valer su título académico en otro país, como la burocracia asociada a validar el título o el considerable fraude existente en materia de títulos académicos.

España, dispone de forma centralizada de todos los títulos oficiales que se expiden en el denominado Registro Nacional de Titulados Universitarios Oficiales (RNTUO), a diferencia de muchos de sus vecinos que almacenan este registro de forma dispersa en las universidades que expiden los títulos. Por ese motivo España se encuentra bien posicionada para conectar con facilidad ese registro RNTUO a la red EBSI de manera que cuando un ciudadano lo solicite se le pueda expedir su título académico en el formato que se está definiendo en EBSI.

Como vemos se trata de un caso de uso que efectivamente resuelve problemas existentes, agiliza las relaciones con administraciones públicas de forma transfronteriza, y facilita que se pueda utilizar también por el sector privado o incluso desde países fuera de la órbita de la Unión Europea.

Una de las posibles conexiones con el mundo privado podría establecerse a través de empresas dedicadas a la búsqueda de empleo como Linkedin, en las cuales los usuarios publicarían su formación académica autorizando a esta red privada a consultar la información que se encuentra en blockchain.

#### 2.12.1.3 El caso de uso "Notarización"

Fue propuesto inicialmente por el Tribunal de Cuentas Europeo en principio para proporcionar a los beneficiarios de fondos y subvenciones europeas un sistema basado en blockchain que permitiera registrar todos los documentos que justifican el gasto de una subvención, típicamente facturas y comprobantes de pago, contratos, etc. De este

modo se facilita la realización de auditorías de manera ágil, transparente, digital y transfronteriza que además se encuentre vinculada al gasto presupuestario de la UE.

Se trata de un registro en la blockchain EBSI que almacena hashes de documentos relevantes y de sus metadatos asociados. Estos hashes son la prueba de autenticidad de documentos que posteriormente se pueden utilizar en una auditoría.

Se pretende que este caso de uso se extienda a todo tipo de documentos, en particular a aquellos que constituyen títulos habilitantes emitidos por administraciones públicas o títulos-valores. Este tipo de documentos están vinculados a un derecho privado patrimonial y hasta ahora sólo existen en soporte papel, porque quien tiene el documento físico también tiene el valor que soporta el documento. En estos casos existen registros centrales donde se realizan las anotaciones respecto a quien es el que posee el documento en cuestión (acciones por ejemplo). Los documentos electrónicos no podían sustituir el soporte papel aunque estuvieran firmados electrónicamente dado que es posible realizar infinitas copias y entregarlas, además sin que el emisor se deshaga del documento electrónico. Como hemos visto, blockchain permite traspasar valor entre entidades, de forma que este problema también se puede resolver gracias a proyectos como el que se está desarrollando en este caso de uso de "Notarización".

### 2.12.2 Otros casos de uso en administraciones públicas utilizando blockchain

#### 2.12.2.1 El registro distribuido de ofertas de contratos del Gobierno de Aragón.

La nueva ley de contratos del sector público[21] obliga a que la presentación de ofertas de contratos a las administraciones públicas se realice de forma electrónica. De momento es obligatoria únicamente la presentación electrónica de las ofertas, aún no lo es la gestión electrónica de todo el procedimiento de contratación. En Aragón era necesario implementar algún sistema de licitaciones electrónicas y tras un análisis de alternativas decidieron acometer un sistema basado en blockchain.

De forma resumida, en las licitaciones públicas el licitador presenta su oferta en un registro, posteriormente las ofertas se abren en un acto público y, una vez abiertas, son valoradas por la mesa de contratación, la cual finalmente envía la propuesta de adjudicación al Órgano de Contratación, el cual procede a firmarla, notificarla y publicarla.

[21] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Esa nueva ley de contratos del sector público ha diseñado específicamente para las licitaciones de una cuantía determinada según el tipo de contrato, un tipo de procedimientos abiertos simplificados y abreviados: art. 159.6 LCSP: "*…c) La oferta se entregará en un único sobre o archivo electrónico y se evaluará, en todo caso, con arreglo a criterios de adjudicación cuantificables mediante la mera aplicación de fórmulas establecidas en los pliegos".* En este tipo de procedimiento descrito no es necesario realizar juicios de valor en los criterios de adjudicación, por lo que la valoración de las ofertas se podrá efectuar automáticamente mediante dispositivos informáticos, o mediante la colaboración de una unidad técnica que auxilie al órgano de contratación.

El Gobierno de Aragón utilizó entonces dos instrumentos jurídicos que tenía a su disposición, en primer lugar la "**actuación administrativa automatizada**", definida en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que permite la producción de actos administrativos con efectos jurídicos sin intervención humana cuando señala en su artículo 41 que *"1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público. 2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación".* En segundo lugar, encontró que en la **Ley de Contratos del Sector Público**, en la **Disposición Adicional 16.1h** se dice que *"en los procedimientos de adjudicación de contratos, el envío por medios electrónicos de las ofertas podrá hacerse en dos fases, transmitiendo primero la huella electrónica de la oferta, con cuya recepción se considerará efectuada su presentación a todos los efectos, y después la oferta propiamente dicha en un plazo máximo de 24 horas. De no efectuarse esta segunda remisión en el plazo indicado, se considerará que la oferta ha sido retirada. Se entiende por huella electrónica de la oferta el conjunto de datos cuyo proceso de generación garantiza que se relacionan de manera inequívoca con el contenido de la oferta propiamente dicha, y que permiten detectar posibles alteraciones del contenido de esta garantizando su integridad. Las copias electrónicas de los documentos que deban incorporarse al expediente, deberán cumplir con lo establecido a tal efecto en la legislación vigente en materia de procedimiento administrativo común, surtiendo los efectos establecidos en la misma".*

Encontramos aquí una definición de lo que es un *hash* en el marco de una ley, lo que ha permitido al Gobierno de Aragón que el licitador registre el *hash* de una oferta en una red de blockchain sin enviar la propia oferta en esta fase de la licitación, ya que es

posible demostrar la existencia de la oferta en el momento en que fue calculado su hash. En este punto, las ventajas de este sistema son que se garantiza el secreto de la oferta, así como hace innecesaria la responsabilidad de custodiar las ofertas en la administración pública hasta que se produce la apertura de plicas ya que no es necesario enviarlas a la administración pública. También permite dinamizar el mercado, ya que cualquiera puede consultar las ofertas (las huellas de las mismas) en tiempo real a medida que van apareciendo en la red de blockchain, cosa que aumenta significativamente la transparencia del procedimiento. Incluso es posible que el mismo licitador envíe más de una oferta, siendo seleccionada siempre para cada licitador la última que haya enviado.

En una primera fase del proyecto, cuando llega la fecha de apertura de plicas, un *smart contract* actúa como mesa de contratación y recibe las ofertas en claro, comprobando que efectivamente no han sido modificadas al comparar los hashes calculados por el propio *smart contract* con los que se encuentran almacenados en la red de blockchain. Si se detecta cualquier diferencia, se deberá a que el licitador, que es el único que ha custodiado la oferta, ha cambiado algo en la misma, y por tanto esa oferta no entrará en consideración.

En una segunda fase, el *smart contract* aplica las fórmulas matemáticas de los pliegos, utilizando los valores correspondientes a los criterios de adjudicación, valorándolos para finalizar proponiendo al adjudicatario, todo ello de una forma completamente automatizada.

#### 2.12.2.2 Zug

Zug es un **pequeño pueblo de Suiza** que ha implementado un **sistema de identidad digital autogestionada basado en Ethereum utilizando una plataforma denominada uPort**. Se han establecido en ese pueblo varias empresas relacionadas con las criptomonedas, dado que Suiza siempre ha sido muy permisivo en el desarrollo de la tecnología financiera, motivo por el cual se conoce a esa zona como *Crypto Valley Zug*.

Los ciudadanos de Zug **pueden realizar algunos trámites con la administración pública utilizando su identidad digital en blockchain** y se está planteando ampliar su uso en el caso de alquiler de bicicletas del ayuntamiento, encuestas y votaciones.

## 2.13 ASPECTOS JURÍDICOS EN RELACIÓN A BLOCKCHAIN

### 2.13.1 Referencias a blockchain en diarios oficiales

**No existe una definición legal sobre blockchain** ni sobre las tecnologías de registro distribuido (DLT). A continuación destacamos sólo algunas de las referencias más relevantes en diarios oficiales a esta tecnología:

- **Resolución de 3 de octubre de 2018, del Parlamento Europeo**, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación 2017/2772(RSP). Esta resolución, entre otras cosas "*Pide a la Comisión y los Estados miembros que desarrollen iniciativas comunes para concienciar y formar a ciudadanos, empresas y administraciones públicas con el fin de facilitar la comprensión y la aceptación de esta tecnología que podría afectar potencialmente a todos los sectores de la economía",* y describe los potenciales efectos en varios sectores" así como *"hace hincapié en que la Unión tiene una excelente oportunidad para convertirse en el líder mundial en el ámbito de la TRD y ser un actor creíble en la configuración de su desarrollo y sus mercados a nivel mundial, en colaboración con sus socios internacionales*".

- **Dictamen del Comité Económico y Social Europeo (CESE)**, publicado el 17 de julio del 2019[22], detalla **varios usos y aplicaciones en diversos sectores utilizando esta tecnología**.
- **Proposición no de ley sobre la introducción de la tecnología blockchain en la Administración Pública en España (Comisión de Economía y Empresa, 22 junio de 2018)[23].**

  "*El Congreso de los Diputados insta al Gobierno a:*

  1. *Introducir la tecnología Blockchain en el sector público español con el objetivo de mejorar los procesos internos y aportar trazabilidad, robustez y transparencia en la toma de decisiones.*
  2. *Desarrollar la tecnología Blockchain en modelos de colaboración pública y privada con el fin de favoreces mercados secundarios de bienes y servicios que abaraten los costes, aumenten la productividad e impulsen la creación de empleo especializado.*
  3. *Facilitar la formación de los recursos humanos en tecnologías Blockchain con el objeto de mejorar al máximo su implantación".*

[22] *DOUE* C 353/1, de 18 de octubre del 2019

[23] http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW12&FMT=INITXDSS.fmt&DOCS=1-1&DOCORDER=FIFO&OPDEF=ADJ&QUERY=%28161%2F003428*.NDOC.%29

- Pregunta al Gobierno (22 de junio de 2018) para su respuesta por escrito (9 octubre de 2018): ¿*Va a desarrollar el Gobierno alguna medida concreta para la introducción de la tecnología blockchain en el ámbito público y privado?* Respuesta: *"…Hay gran número de casos de uso en la Administración Pública que podrían beneficiarse de las características inherentes de estas tecnologías, entre ellos: identidad digital, registros, voto, historial de ayudas, etc. Los procedimientos administrativos, tanto internos como externos, en los que concurren más de un departamento pueden beneficiarse especialmente de estas tecnologías…".*[24]

- **Real Decreto-Ley 14/2019**, **por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.** Es la primera norma jurídica que menciona a esta tecnología, en este caso para prohibir su uso en el ámbito de las administraciones públicas en su disposición adicional sexta cuando señala que "***no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados,*** *los* ***sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea***". Esta disposición hace referencia a los sistemas de identidad autogestionada que han sido descritos anteriormente.

### 2.13.2 Blockchain y protección de datos personales

Dado que el registro en blockchain es inmutable, es necesario diseñar modelos compatibles con el derecho al olvido; asimismo también es necesario que la información en la cadena de bloques esté lo suficientemente anonimizada como para que no sea posible identificar a las personas. Por ese motivo, **cada proyecto blockchain requerirá de un análisis de riesgos en términos de la protección de datos que determine si existe una protección adecuada de los derechos de los usuarios en términos del RGPD**. Por ejemplo, no basta utilizar *hashes* como método de anonimización *per sé*, sino que hay que analizar si el método utilizado para generar esos *hashes* es realmente seguro e impide, por ejemplo, la realización de perfiles de usuario recorriendo la información contenida en blockchain.

[24] http://www.congreso.es/l12p/e10/e_0105876_n_000.pdf

### 2.13.3 KYC y AML

**Know Your Customer – KYC (conoce tu cliente) y Anti Money Laundering – AML (prevención de blanqueo de capitales) son procesos establecidos legalmente que han de cumplir las empresas para verificar la identidad de sus clientes y para procurar evitar actividades ilegales relacionadas con el blanqueo de dinero.** Además de cerciorarse de la identidad del cliente con una comprobación de documentos, es necesario ir más allá para cerciorarse de esa identidad de los clientes y compartir esa información con la administración de cara a evitar el fraude y la suplantación de identidad.

Para evitar esas actividades ilegales, muchos gobiernos han legislado y establecido procedimientos que aumentan los controles que han de realizar las empresas en estos ámbitos, normalmente empresas del sector bancario, asegurador, criptomonedas, juego online o apuestas entre otras. En Europa existe la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. Se trata de una directiva dirigida al sector financiero y pretende establecer las medidas que permitan a los bancos defenderse de este tipo de amenazas que se suele denominar como 5AML.

Esta directiva **obliga a la identificación completa de ciertos usuarios que antes podían ser anónimos** en el sector bancario y financiero, **en concreto también han de identificarse los usuarios en relación con el tráfico y uso de las criptomonedas**.

Existen **varias iniciativas en las cuales la tecnología blockchain precisamente ayuda a dar cumplimiento de estos procedimientos** en proyectos que utilizan sistemas de identidad autogestionada.