UNIVERSIDAD DE ZARAGOZA

FACULTAD DE DERECHO

TRABAJO DE FIN DE GRADO

LA APLICACIÓN DE LA BLOCKCHAIN POR LA ADMINISTRACIÓN PÚBLICA

COMPRENSIÓN GENERAL DE SU IMPLEMENTACIÓN

Yandy Abel Candelario Vallejo

Grado en Derecho. Grupo 42

Curso 2021/2022

TUTOR ACADÉMICO

MIGUEL ANGEL BERNAL BLEY, PROFESOR TITULAR DE DERECHO ADMINISTRATIVO DE LA UNIVERSIDAD DE ZARAGOZA

RESUMEN: Este trabajo de fin de grado muestra un análisis en el marco actual de la administración pública sobre el cual poder integrar sistemas tecnológicos basados en Blockchain. El análisis se da tanto en legislación nacional como europea concerniente a la primera, mostrando las barreras y requisitos legales que debería superar la administración pública en un plano europeo para su implementación. Explorando en concreto la utilidad de la Identidad Soberana Digital y presentando una idea de colaboración con la herramienta ya existente y en funcionamiento de la UE.

ÍNDICE

LISTADO DE ABREVIATURAS UTILIZADAS

DLT	*Distributed Ledger Technology*
P2P	*Peer-to-peer*
RSA	*Rivest–Shamir–Adleman*
API	*Application Programming Interfaces*
EBSI	*European Blockchain Services Infrastructure*
DNI	*Documento Nacional de Identidad*

I. INTRODUCCIÓN

1. CUESTIÓN TRATADA

Previo cualquier ahondamiento creo pertinente entender cuál es el objetivo general de este trabajo, siendo este en grandes rasgos la informatización de la administración pública. Esto es la administración electrónica, de esta se han dado numerosas definiciones en tanto que ha surgido a la par con las nuevas tecnologías y cada país lo entiende de una forma distinta pero no distante uno de otro. Así pues y de acuerdo a la Unión Europea, podemos entenderlo como un conjunto de medidas que exploran los beneficios de las tecnologías de la información con el objetivo de desarrollar en el sector público formas de ofrecer sus servicios a los ciudadanos, reduciendo de paso costes y mejorando su eficiencia (Comisión Europea , 2010).

En concreto ahondaremos en una nueva tecnología con un gran potencial para ser parte de la administración electrónica del futuro. Esta es la Blockchain, tecnología innovadora de las últimas dos décadas que ha llevado a una revolución monetaria. La mayoría de la población la conoce por la invención del *Bitcoin*, sin saber que esta es uno de los múltiples y muy variados usos de esta tecnología, influenciando el ámbito monetario y capaz igualmente de revolucionar la administración pública, sanitaria, bancaria, y la manera en la que el ciudadano interactúa con una administración no solo más eficiente, sino también segura y económica.

En el cuerpo del mismo, presentaré tanto las definiciones básicas alrededor de la *Blockchain*, algunos de los tipos de esta que existen (y son pertinentes para el uso que pretendemos obtener de esta al caso de este trabajo). Seguido por su lugar en la legislación básica de nuestra administración pública, la implementación que desde este trabajo se anima a realizar en el sector público junto con su precedente europeo y en último lugar los problemas legales que aún están por resolverse respecto a esta implementación.

2. RAZÓN DE LA ELECCIÓN DEL TEMA

Desde infante siempre he tenido una relación especial con la tecnología, a mis 4 años ya podía manejar un ordenador de manera básica, siendo este donde pasaría una gran parte de mi tiempo libre. Este amor por la tecnología y lo digital es uno especial que ha seguido creciendo a medida que lo he hecho yo, manifestándose en diferentes vías, siendo una de ellas el Derecho.

En muy poco tiempo, 20 años aproximadamente, el mundo ha cambiado radicalmente gracias a una fuerte globalización y un mucho más fácil acceso al internet hasta el punto en el que no solo es una herramienta, sino que constituye una autentica necesidad que abarca desde la educación hasta el ámbito laboral y social, siendo este a través de dispositivos móviles nuestro principal medio de comunicación. Así como ha evolucionado la forma en la que nos comunicamos e interactuamos con los ámbitos productivos de nuestra sociedad, debería desarrollarse la administración pública. El sector privado y nuestra manera de consumir se ha digitalizado considerablemente, siendo este en varios ámbitos el principal medio de no solo comprar bienes físicos si no también ítems digitales.

Es en este punto en el que mi pasión por el Derecho y la tecnología se cruzan, buscando una forma de que el Estado pueda seguir el paso no solo a los avances tecnológicos que cada vez son más una necesidad que un lujo, sino a la sociedad que se desenvuelve con ellos. Hayo apasionante el poder explorar y sentar pie en la base que será la administración del futuro, donde podamos no solo interactuar con una administración auténticamente moderna, sino tan confiables como nosotros mismos. Y sí de confianza se trata, es donde la *Blockchain* se lleva el oro, aportándonos un sistema gracias al cual podemos dejar de dudar y tomar la administración como un ente tercero, ajeno o incluso contrario a nosotros, para pasar a formar parte de la misma tanto implícita y explícitamente, velando por nuestros intereses y derechos a través de las redes.

Para ello claro es importante que estudiemos esta nueva tecnología, viendo las formas en las que podemos implementarla y los tipos que más benefician a la administración pública para con los ciudadanos. Es por ello que este trabajo apunta a avivar un poco el fuego que otros ya han empezado, aportar un poco más de leña al fuego de la evolución que representa la administración electrónica.

3. METODOLOGÍA SEGUIDA

Para la elaboración de este escrito, principalmente me he servido de una variedad de fuentes expertas en materia de *Blockchain* con el objetivo de ver y extrapolar las conclusiones más importantes en los intentos y proyectos que se están realizando a nivel europeo. Por ello las fuentes mas revisadas son aquellas realizadas por los diferentes grupos de trabajo comisionados por la comisión europea, una serie de investigaciones en materia de *Blockchain* de las distintas universidades del mundo y en último lugar nuestra legislación vigente para su contraste.

II. BLOCKCHAIN

1. CONOCIMIENTO PREVIO, *DLTs*

Sí bien la Blockchain ha ganado un gran impulso en el sector financiero y socialmente la relacionamos casi exclusivamente al *Bitcoin*, en los últimos años se ha empezado a aplicar esta tecnología a otros sectores que podrían beneficiarse de ella. Principalmente veremos el potencial que esta tecnología tiene como una infraestructura de información.

La tecnología de *Blockchain* no es una creación totalmente nueva, en lo que a las partes que la configuran respecta, sino que tratamos tecnologías ya existentes entrelazadas entre si de una forma muy especial y concreta con la capacidad de crear redes basadas en la confianza entre partes que en un principio no tienen razón alguna para confiar.

Para ello creo pertinente definir primer las distintas tecnologías que componen el núcleo de esta.

En primera instancia nos encontramos con la *Distributed Ledger Technology (DLT) o* Tecnología de Libro Mayor Distribuido. Cabe recalcar que una *DLT* no es per sé parte de una *Blockchain*, si no que la *Blockchain* es una *DLT* con características muy concretas. Teniendo esto en mente, podríamos definir la *DLT* como un consenso compartido y sincronizado de datos (que nos dice quién es el propietario de cierta cantidad de dinero, un bien físico, el contenido de un camión de transportes…) distribuidos entre múltiples usuarios (dispositivos) en distintas localizaciones. Su fundamentación principal descansa en que todos los usuarios tienen una copia idéntica del dato en cuestión, de manera que una vez la mayoría de los usuarios tengan el mismo dato confirmando, dicho dato se tenga por veraz y por lo tanto se verifique, encripte y guarde cronológicamente.

Para poder acceder a la misma necesitaremos una llave. Estas tienen distintas propiedades para usos concretos, pudiendo ser tanto para modificar (pongamos por ejemplo una llave dada a un organismo judicial para lo que le compete) como para únicamente ver las transacciones/datos que se tienen por veraces (ciudadano que revisa los datos).

Como estos datos pueden ser revisados, se encuentran divididos en diversos lugares (que dependiendo del tipo de red puede ser el dispositivo del usuario o en nodos) y necesita que la mayoría de estas copias se modifiquen para que un dato quede validado y registrado, se garantiza en gran medida la transparencia y la seguridad (sería necesario e imposible hackear a la mayoría de los usuarios que poseen una copia). (UK Government Chief Scientific Adviser, 2016)

Profundizando un poco más en el aspecto de los usuarios que hemos visto en la *DLT*, cabe ver cómo funcionan estos. Los datos como hemos dicho están repartidos entre distintos usuarios (dispositivos) que se comunican de una manera muy específica. Estos dispositivos pueden ser ordenadores, siendo estos donde guardaremos la copia que se comparte y repite de los tantos alrededores del mundo conectados a la misma red, adquiriendo así la definición de **Nodo**, los cuales se comunican entre si mediante un protocolo de *P2P (Peer-to-Peer o* Red entre Iguales*)*.

Para entender el *P2P*, vamos a verlo primero de forma independiente y posteriormente aplicado al caso. Esta es una tecnología que lleva con nosotros mucho tiempo, quizá la conozcamos en otras formas como en aplicaciones de principios del año 2000 como «*Napster»*, *«Utorrent»* o «*emule»* entre otros. Mediante estas aplicaciones era posible la imparable piratería gracias a este protocolo (quizá no en la mejor forma, pero ya podemos ver la gran aplicación de esta descentralización ante la imposibilidad de manipular directamente los datos por un tercero no deseado). En este caso prescindíamos de un sistema centralizado o un servidor que guardase y distribuyese los datos, pues los usuarios utilizaban sus propios dispositivos, poder de computación, ancho de banda y datos para compartir entre ellos de forma directa los archivos que precisaban (música, películas, etc…), careciendo de la necesidad de un servidor en el que alojar los datos compartidos.

En un principio podíamos encontrar P2P conexiones que si requerían de un servidor como punto de enlace, siendo posible a día de hoy un P2P totalmente descentralizado creando una conexión directa entre nodos o incluso hibrida donde se sigue usando el servidor con el único fin de manejar los recursos y encaminar la información pero sin almacenarla.

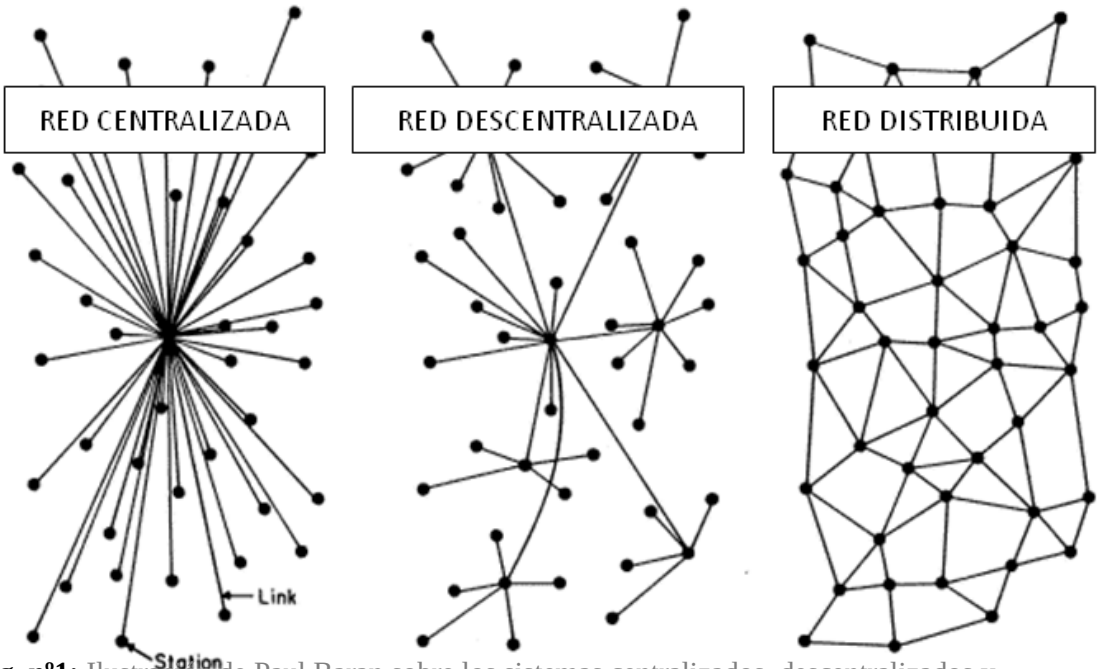


Fig. nº1: Ilustración de Paul Baran sobre los sistemas centralizados, descentralizados y distribuidos (Baran, 1964)

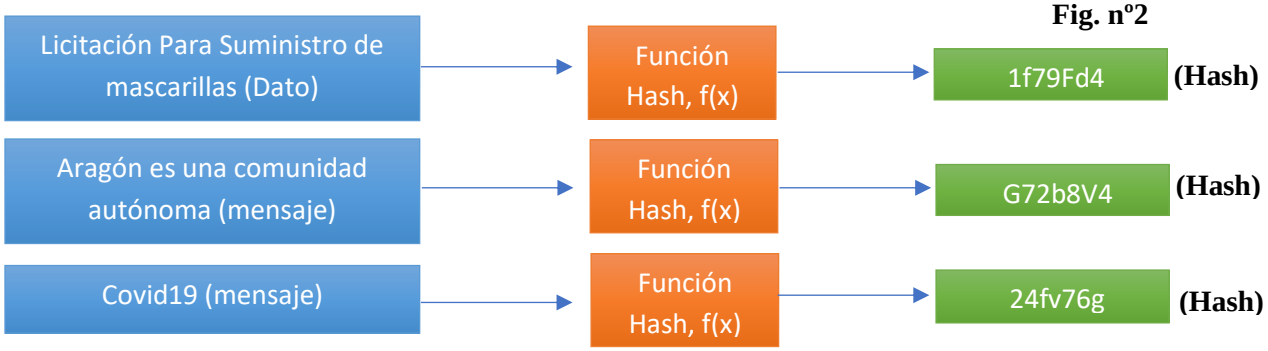
Con este concepto más simple podemos entender cómo funciona el P2P descentralizado dentro de la DLT o Blockchain, pues como sistema principalmente descentralizado (donde reside el fuerte de la transparencia y seguridad ya mencionados) permite una conexión directa a la red mediante la cual se verifican y guardan los datos, red constituida por las copias encriptadas que cada usuario en su nodo (ordenador o dispositivo análogo) guarda y comparte al mismo tiempo con los demás nodos (usuarios).

2. CONOCIMIENTO PREVIO, Hash Criptográfico

Retrocediendo un paso atrás para avanzar dos, es necesario que antes de abarcar la definición de este apartado, conozcamos lo que es una función *hash*.

Una función *hash* es un algoritmo que convierte un mensaje o dato de extensión indeterminada en un resultado de extensión fija. En este proceso de conversión lo que este algoritmo hará es no solo «traducir» o «identificar» cierto mensaje si no al mismo tiempo indexarlo. Produciendo de esta manera un resultado de extensión mucho menor, ocupando menos espacio, de dificultad reducida para computar y manejar (Aerts, 2011)

Fig. nº2



Como podemos ver en la Fig. nº1, independientemente de si aquello que tratamos en nuestra *DLT* o *Blockchain* es un dato como puede ser un contrato de licitación en toda su extensión como mensajes de distinto tamaño, siempre obtendremos un valor alfanumérico (si así ha sido programada la función) de extensión limitada con el cual identificaremos ese mensaje o dato(s) que en el proceso habrán sido indexados por la función para su posterior reconocimiento.

Sabiendo lo que es una función *hash*, podemos ahora entender el concepto de función criptográfica de *hash*, mientras que las funciones de *hash* como la anteriormente expuesta se utilizan como un sistema de búsqueda, de la misma forma en la que buscamos en un índice o un diccionario, las funciones criptográficas de *hash* se caracterizan por ser de vía única, es decir, su objetivo es hacer posible obtener el *hash* a partir del mensaje o dato e imposible obtener el dato a partir del *hash*. (Aerts, 2011) Como comprenderemos igualmente, el *hash* corresponde a ese mensaje compuesto por caracteres y orden específicos, a esta representación la llamamos *Fingerprint*, lo cual ya nos da una primera cota de seguridad sabiendo que la creación de ese hash se da por la persona que crea o escribe el mensaje/dato.

El hash más usado dentro de la *Blockchain*, entre otras aplicaciones es el *SHA-256*, debido a su mayor facilidad de aplicación e incremento de seguridad, ya que, con la adición de más bits, se hace considerablemente más difícil inferir su contenido original. Siendo homólogo de este tenemos el *SHA-512*, el cual aumenta considerablemente la seguridad, con la consecuencia de una perdida en agilidad, el uso quedará reservado a cuanto que primemos más. (Halil Saltik, 2022)

3. CONOCIMIENTO PREVIO, Criptografía Asimétrica/De Clave Pública

Es posible que el con confundamos el *hash* con la criptografía, pero es importante notar que ambas si bien se compenetran no son lo mismo. El ámbito de la criptografía es bastante amplio, pero para el caso que nos compete únicamente miraremos la criptografía asimétrica. La cual corresponde a la necesidad de confidencialidad y seguridad.

Entendemos la criptografía como la práctica de una técnica para una comunicación segura mediante la encriptación, siendo esta como el proceso de codificar un mensaje o información en otro distinto ilegible para todos excepto las partes pertinentes (remitente y receptor) (Baldegger Rico, 2019). En la actualidad la criptografía es un área estrechamente enlazada a la computación e ingeniería informática, de manera que buscamos crear algoritmos matemáticos extremadamente difíciles de resolver que si bien no son imposibles con fuerza bruta si son terriblemente ineficaces pues podríamos tardar más de una vida entera para descifrarlo.

Generalmente para que el receptor pueda comprender el mensaje encriptado es necesario que conozca la técnica a través de la cual el remitente ha encriptado el mensaje, de manera que pueda desvelar su contenido, obteniendo como prueba de su veracidad el conocimiento exclusivo en la técnica de codificación compartido entre él y el remitente.

En este caso la criptografía asimétrica o criptografía de clave publica, consiste en la encriptación del mensaje o archivo mediante algoritmos matemáticas muy complejos basados en funciones de vía única (mismo termino que el explicado anteriormente con el hash criptográfico) junto al cual se expiden dos llaves mediante algoritmos RSA. Una de ellas es pública (usada para encriptar) y una clave privada (para desencriptar), no siendo posible averiguar una llave (código alfanumérico) a partir de la otra.

Para este uso concreto vemos que es necesario que remitente y receptor ambos revelen o envíen sus claves publicas entre sí. De manera que A podrá encriptar un mensaje con la clave pública de B, de forma que B pueda desencriptarlo con su clave privada. Todo el mundo que conozca de la clave publica de B podrá encriptar mensajes para él, pero nada más. Siendo el núcleo de esta seguridad el mantener la llave privada bajo secreto siendo B el único que la sepa.

4. CONOCIMIENTO PREVIO, Contrato Inteligente/Smart Contract

El contrato inteligente lo entendemos como un programa que reside dentro de la *DLT* diseñado para ejecutar, controlar o documentar legalmente de forma automática acciones en los mismos términos de un contrato o acuerdo (Szabo, 1997)

Al igual que con las *DLT,* el objetivo de la firma inteligente es prescindir de un tercero que nos proporcione la seguridad y confianza que de otra forma no tendríamos respecto a la contraparte firmante. Hay que prestar atención en que no son la misma tecnología aun si se retroalimentan, pues la *DLT* es el ecosistema en el que principalmente haremos uso de la firma electrónica y dónde quede registrado el uso de la misma con un sello temporal.

Este programa en concreto reside dentro de esa cadena de datos que quedan guardados y verificados en la *DLT* tras llegar al consenso, dotando de gran seguridad e inmutabilidad el contrato que acabamos de realizar. La red más popular para realizar estos contratos por su versatilidad la encontramos en el *Ethereum*, red de *Blockchain* (y de forma última una *DLT*) con su propia criptomoneda, siendo esta una pero no la única característica de esta red multitareas.

Así pues, podemos programar un contrato inteligente con una serie de parámetros como puede ser por ejemplo para una licitación, en la que la administración pública ponga a disposición el dinero preciso y hasta que no se realice el objeto del contrato en los términos estipulados, dichos fondos no podrán ser accesibles o manipulados. Siendo este un proceso totalmente automático e inmutable que aporta a ambas partes seguridad en lo que a sus intereses respecta.

5. CONOCIMIENTO PREVIO, Firma Inteligente/Digital Signature

Aplicando todo lo explicado tanto en lo respecto a la criptografía asimétrica o de clave publica, así como el concepto de *hash* y funciones *hash*, en un solo punto, podemos entender plenamente el significado o el contenido de esta nueva tecnología de firma inteligente.

En primer lugar entender que la firma inteligente es una de las aplicaciones principales de la criptográfica asimétrica, en tanto que es un mecanismo criptográfico que tiene como fin asegurar al receptor de un documento digitalmente firmado que el remitente es quien dice ser (pudiendo ser un usuario o una entidad gubernamental) (Branstad, 1983), dándonos pues autentificación y no repudio pues como hemos visto con esta tecnología permite que nos llegue el documento sin alteración alguna.

Desde una perspectiva más técnica, tenemos el mismo procedimiento que hemos visto anteriormente con la criptografía asimétrica. Basándose principalmente en tres algoritmos. El primero de ellos el correspondiente al núcleo de la criptografía asimétrica, otorgándonos una clave privada y una pública. El segundo es el algoritmo de firma, que teniendo un mensaje (nuestra firma) y la clave privada produce esa marca o sello digital que consideramos firma. Y en tercer lugar el algoritmo de verificación para el usaremos la clave pública, de forma que con introducir la clave publica que nos ha conferido el remitente, el programa nos dirá que «acepta» o «repudia» dicha clave. Siendo para cada caso la manera de autentificar si quien envía y firma ese documento es quien dice ser.

De una manera más simplificada, la firma digital vinculará a una persona o entidad con un documento en concreto, dándose que la firma se corresponderá con una identidad en específico, siendo esta la única que posea la clave privada.

En lo que respecta a la utilidad del *hash* o función *hash* vemos que se aplica a la seguridad. Lo que sucederá es que, de forma previa a la emisión de la firma con la clave privada, ejecutemos una función *hash* a dicha firma, de forma que de la misma obtengamos una «etiqueta» alfanumérica que efectivamente se corresponda con dicha firma/dato. Y encima de esta capa pongamos nuestra firma inteligente.

Recordemos que el *hash* criptográfico hace que sea imposible encontrar el análogo dato o documento original a partir del *hash*, por lo que aún si la ya improbable firma encriptada fuese objeto de un ataque de fuerza bruta (donde un programa intenta crear o adivinar la clave a partir de una serie de parámetros a una velocidad moderada) esta solo emita o deje

al alcance el *hash*, no pudiendo manipular ni interactuar directamente con el mensaje o dato, siendo en este caso nuestra firma.

Este método que acabamos de describir corresponde al tipo de firma *RSA*, que corresponde con el mismo tipo de algoritmo en el que se basa la criptografía asimétrica. Cabe mencionar que hay una varia gama de estas con sus funciones propias, sin embargo, por el tema y mera necesidad de comprensión general del concepto, no se profundizará en ellas.

Cabe recalcar que, aunque esta tecnología suene extemporánea, es algo presente y cada vez más utilizado. Actualmente estas tienen validez legal con lo dispuesto en el Art. 26 del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (eIDAS), se nos da una serie de criterios con los que una firma digital tendrá total validez legal. Precisando pues que esta se identifique únicamente con un individuo, permitir la identificación del firmante (modelo RSA con Clave pública), haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

6. BLOCKCHAIN

Como hemos dicho anteriormente, la *Blockchain* es un tipo concreto de *DLT*, de estas existen una gran variedad de tipos para los distintos casos de uso, comerciales, financieras, privadas y entre otras la que más nos conviene, el sector público.

La *Blockchain* tomó su gran impulso al público por primera vez en 2008 de la mano del *Bitcoin* por Satoshi Nakamoto (Seudónimo)

Es una estructura de datos distribuido comprimida en una cadena de bloques. La *Blockchain* actúa bajo el concepto anteriormente visto de *DLT*, siendo los datos que en ella se guardan y encriptan registros de todas las transacciones en la red de *Blockchain*. Las transacciones están etiquetadas con una estampa temporal y agrupadas en bloques donde cada bloque se ve identificado por un *hash* criptográfico. Los bloques forman una secuencia linear de manera que cada bloque referencia el hash del anterior, formando una cadena de bloques. Esta esta mantenida por una red de nodos (dispositivos) y cada nodo ejecuta y graba las mismas transacciones, de manera que existe una copia en cada uno de los dispositivos, replicándose entre todos los nodos, siendo capaz para cada uno de estos el leer las transacciones. (Arshdeep Bahga, 2016)

Con una idea generalizada de la misma, habiendo comprendido los conceptos anteriores y que es la Blockchain, podemos ver los tipos de la misma que podemos encontrar en la Fig. nº3.

Fig. nº3

			LEER	ESCRIBIR	COMPROMISO	EJEMPLOS
TIPOS DE BLOCKCHAIN	ABIERTA	Pública sin permisos	Abierta a cualquiera	Cualquiera	Cualquiera	Bitcóin y Ethereum
		Pública con permisos	Abierta a cualquiera	Participantes autorizados	Todos o parte de los participantes autorizados	Libro de la cadena de suministro visible al público
	CERRADA	Consorcio	Restringido a un grupo autorizado de participantes	Participantes autorizados	Todos o parte de los participantes autorizados	Múltiples bancos que operan un libro de contabilidad compartido
		Empresa privada autorizada	Totalmente privada o restringida a un conjunto limitado de nodos autorizados	Sólo para operadores de red	Sólo para operadores de red	Libro externo de cuentas bancarias compartido entre la sociedad matriz y las subsidiarias

Fuente: Hileman & Rauchs, 2017

III. EL MARCO LEGAL ACTUAL

Ahora que comprendemos de forma extensiva en que se basa la tecnología que pretendemos incluir e integrar de manera simbiótica a nuestra administración pública, es pertinente entender como segundo paso donde encaja esta en la legislación actual. De esta manera podemos deslumbrar de una manera clara y precisa cuanto puede operar esta tecnología en nuestro sector público sin toparse con impedimentos de carácter legal. Poniendo énfasis en donde es necesario tirar muros legislativos para levantar nuevos acordes a los tiempos tan rápidos en los que vivimos.

Lo primero que cabe notar en este aspecto es que en la presente legislación actual en algunos de los sectores públicos lo único que hemos hecho es digitalizar la burocracia que podríamos definir como poco flexible y ágil, todo lo contrario, a lo que apuntamos a conseguir (Carranza, 2021).

1. LA BASE DE NUESTRO PROCEDIMIENTO ADMINISTRATIVO

Más adelante se expondrá con mayor detalle una *Blockchain* concreta con un objetivo específico que buscará crecer en cuanto a lo que es capaz de hacer. Sin embargo, para poder establecer el marco legal de la misma, creo necesario primero establecer el núcleo que compone esta idea, siendo esta la *Blockchain* y el conjunto de tecnologías de las que está compuesta como se ha explicado en el primer apartado. Un sistema de cadena de bloques descentralizada y pública principalmente en manos del estado y ciudadanos identificados en esta misma.

El primer sector en el que considero esencial ver la compatibilidad de esta nueva tecnología es tanto el procedimiento administrativo (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas de 2015) y el régimen jurídico (Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público de 2015).

Adentrándonos en la Ley 39/2015 nos encontramos con que a pesar de dejar lo que parece ser una vía abierta para que los ciudadanos se identifiquen electrónicamente con las administraciones públicas en su art 9.2.C):

«Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes […] **Cualquier otro sistema** que las Administraciones

públicas consideren válido en los términos y condiciones que se establezca, **siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación** a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. **Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente**. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud»

Refiriéndose igual en los mismos términos en lo que se refiere a la firma electrónica en su art 10.2.C), dando espacio a «**cualquier otro sistema que las administraciones públicas consideren válido»**. Lamentablemente debido al Real Decreto-ley de 2019, cuyo motivo aparente es el de establecer un marco normativo por el que se comprendan medidas de contacto e identificación con la administración pública, es el principal bloque de oposición hacia una innovación tecnológica. Así pues, en su disposición adicional sexta, se prohíbe el uso de toda tecnología Blockchain:

«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…»

Todo esto es claro en lo referido a la Ley 39/2015, sin embargo, ya nos pone una traba lo suficientemente poderosa como para hacer perecedero todo el sistema, pues sin la identificación y la posibilidad de firmar es esencialmente imposible establecer un sistema con el que el ciudadano pueda comunicarse no solo con la administración pública, sino también con terceros en relación a esta.

2. LA BASE DE REGIMEN ADMINISTRATIVO

En una segunda instancia nos encontramos con el régimen jurídico establecido en la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público, con especial énfasis en los artículos 40 a 46 bis, donde se regula todo lo referente a la administración electrónica.

Es importante notar que, si bien la Ley 40/2015 no es apropiada para la regulación de la Blockchain, ni su actual redacción permite una efectiva regulación de esta tecnología. Lo pretendido en las siguientes paginas es mostrar la capacidad que la Blockchain tiene para cumplir con los requisitos de la tecnología ya establecida. Es decir, cumple con el espíritu de funcionamiento con el que se redactó la legislación.

De entre los diversos artículos en esta ley, cabe remarcar una serie de ellos empezando por el artículo 40, permitiendo la identificación de las administraciones públicas «mediante el uso de un **sello electrónico** basado en un certificado electrónico reconocido **o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica**.” Al tiempo que se nos requiere: “**la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos**. **La relación de sellos electrónicos utilizados** por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, **deberá ser pública y accesible por medios electrónicos.** Además, **cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos**»

Haciendo un pequeño análisis vemos pues que en tanto que reuniésemos los requisitos precisos de firma electrónica que podemos encontrar en el Reglamento (UE) no 910/2014: relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior [Reglamento eIDAS]. Se nos permitiría el uso de sellos electrónicos cualificados, que de acuerdo al artículos 26, 28 y anexo I del reglamento eIDAS precisaría de «a) estar vinculada al firmante **de manera única**; b) **permitir la identificación del firmante**; c) haber sido creada utilizando datos de creación de la firma electrónica **que el firmante puede utilizar**, con un **alto nivel de confianza, bajo su control exclusivo**, y d) estar vinculada con los datos firmados por la misma **de modo tal que cualquier modificación ulterior de los mismos sea detectable.»**

Todos estos requisitos que bien se nos presentan para su uso por parte de la administración pública son elementos inherentes y naturales de la *Blockchain*, permitiendo no solo su identificación si no también su vínculo único a dicha firma mediante el *hash* y la criptografía asimétrica. En tanto que, el *hash* por su naturaleza ha de ser único y la criptografía asimétrica

permite al usuario ser el único en tener la clave privada, así como su uso con un alto nivel de confianza, dando así con el no repudio que se nos pide.

De movernos un poco más en su anexo I, se nos da una serie de datos más que cualidades de las que ha de dotarse la firma de contenido, de la misma manera en la que hemos visto cómo podemos transformar mensajes y documentos en un *hash* y engravarlo en un bloque, es igual de posible que esta tenga igual o mayor contenido del que se nos pide.

Igualmente, la verificación y transparencia se encontraría garantizada en todo momento, pues es posible el realizar un portal web a través del cual ver todos los movimientos de la *Blockchain*, de la misma manera en la que se realizó en la implementación que tuvo lugar en Aragón en el ámbito de la contratación pública mediante su propio visor público de la *Blockchain.*

Siguiendo con los artículos de la Ley 40/2015 nos topamos con un artículo esencial que es el artículo 41 relativo a la actuación automatizada de la administración. De acuerdo a este artículo se entenderá 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»

Si bien su definición encaja a la perfección con el cometido que pretendemos con la *Blockchain,* su numeral segundo es el más relevante. Estableciéndonos que órganos y especificaciones técnicas deberán seguirse para su correcto funcionamiento administrativo, constando con un órgano de impugnación. Podríamos entender como posibilidad para esta nueva tecnología que fuere responsabilidad de la Agencia Estatal de Administración Digital (AEAD) creada a partir de la Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022. Entendiendo que el objeto descrito de la misma en la disposición adicional 117ª es principalmente la digitalización y transformación digital del sector público.

En lo que respecta a los siguientes preceptos, se abordan cuestiones relativas a los sistemas de firma para la actuación administrativa automatizada (artículo 42), la Firma electrónica del personal al servicio de las Administraciones Públicas (artículo 43) e Intercambio electrónico de datos en entornos cerrados de comunicación (artículo 44).

En lo referido al artículo 42 únicamente se nos hace referencia a la posibilidad de las administraciones públicas de determinar sus supuestos de uso, así como su verificación mediante código seguro (que como ya hemos visto no sería preciso con la doble funcionalidad del *hash* anteriormente mencionada). Para el artículo 43 trata el uso por parte del funcionariado de dicha firma siempre que utilice medios electrónicos (posible mediante la creación de una firma electrónica única a esa posición y funcionario). En última instancia para el artículo 44 remarcamos su subapartado 4º, pues prima la seguridad del entorno cerrado de comunicaciones y los datos que en ella se transmitan (siendo este el uso principal que como hemos visto obtenemos de la criptografía asimétrica).

En una vista especial, contamos con el artículo 45, referidos al aseguramiento de la interoperabilidad de la firma electrónica, más aún aquellos distintos a los de otras administraciones, pudiendo estas superponer un sello electrónico propio de su sistema sobre el archivo en específico. Y en última instancia el artículo 46 y 46 bis, destacando el ahínco que en el artículo 46.2 se da a la seguridad: «asegurarán la **identificación de los usuarios** y el **control de accesos**, el cumplimiento de las **garantías previstas en la legislación de protección de datos**, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran»

En este punto me gustaría una vez más poner en relación a la *Blockchain*, el control de acceso como bien se nos pide en la legislación puede realizarse mediante la construcción de una *Blockchain* pública permisionada (*vid.* Fig. 3ª), en tanto que no solo permite la participación de terceros usuarios (como queremos que sea para la ciudadanía) pero cerrándose a ciertas vulnerabilidades y siendo transparente en lo justo con el fin de un plus añadido de seguridad.

En lo referente a la protección de datos, para el correcto alineamiento con nuestra 40/2015, se explicará más adelante.

3. REQUISITOS GENERALES SOLICITADOS

Entiendo pertinente mencionar la Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.

Si bien al sistema al que nos estamos refiriendo es una firma criptográfica, distinto a este, es pertinente que estas realicen la tarea que hasta ahora las no criptográficas venían realizando, poniendo de relieve la necesidad para una nueva regulación que no se rija con el mero propósito de «digitalizar».

En primer lugar, entiendo pertinente mencionar la categorización de categoría básica que se requiere del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Debido a las diferencias existentes en firmas criptográficas basadas en Blockchain con el sistema actual, creo que sería pertinente no encajarlo todo en este sistema de medición de seguridad. Al tratarse de sistemas distintos, lo pertinente a mi criterio seria crear su propia regulación y modificar el actual ENS, no solo para este sistema concreto (ni solo por las diferencias) si no para todas aquellas firmas criptográficas y aplicaciones que puedan surgir basadas en un sistema *Blockchain* que permita una rápida implementación sin demasiados cambios jurídicos.

Es precisamente la mutabilidad de esta "nueva" tecnología lo que se usa como escudo por una legislación y regulación propia debido a la dificultad que entraña el asentar bases sobre tecnología falta de madurez. Sin embargo, aquello que tantos ven de forma negativa en torno al marco jurídico, es una oportunidad, ya que la intervención en una época temprana por parte de los poderes públicos es esencial para garantizar que su futuro desarrollo respetará los principios jurídicos esenciales del ordenamiento y consecuentemente el de los ciudadanos (Finck, 2019). Tenemos la oportunidad de que en vez de ser ex post que el derecho se desarrolle, sea ex ante, impulsando una tecnología a madurar con las bases y principios del marco regulatorio español.

En lo que al resto de requisitos respecta, vemos que precisa no solo de la integridad de la firma realizada, sino también de la información y documentos presentes en el proceso junto a un sello temporal con su incorporación inmediata al sistema de información asociado a dicho procedimiento. Asegurando en todo momento que se no se de repudio alguno. Todo esto seguido por una forma de garantizar el consentimiento del interesado mediante el sistema clave.

Una vez más vemos como por el inherente funcionamiento del núcleo de lo que constituye la *Blockchain*, podemos garantizar la integridad no solo de la firma (clave criptográfica), sino también de los documentos que se han presentado (inmutabilidad de la Blockchain con el fácil acceso de búsqueda aparejado a esta), el no repudio y el garantizar el consentimiento

son dos características que vendrán de la mano del *hash* y la clave privada propia de la *criptografía asimétrica*. Recordemos que tanto el hash como la clave privada son elementos que principalmente y de modo quasi-exclusivo para el *hash* (con el cual se identifique esa carpeta ciudadana) y exclusivo para la clave, conocerá únicamente la persona física que en el proceso concreto precise de la realización de un acto administrativo. Garantizando el no repudio gracias al sistema de clave pública.

4. EL ANTECEDENTE DE ARAGÓN

Dentro de las entrañas del derecho administrativo nos encontramos con un precedente en materia de *Blockchain*, que no solo consiguió una adaptación técnica a la administración sino también legal con resultados muy prometedores para proyectos similares en el futuro.

En este caso me refiero al proceso administrativo de contratación pública mediante *Blockchain* llevado a cabo por el Gobierno de Aragón. En lo que respecta a su base legal, tomamos prestada el ya mencionado artículo 41 LRJSP, acompañado del artículo 159.6.d), el cual nos garantiza en el procedimiento abierto simplificado que no se realizará la apertura de las proposiciones hasta que su plazo de presentación haya finalizado.

Para conseguir una comunicación entre licitante y licitador inequívoca e inalterable se sirvió de la huella electrónica mediante *Blockchain*, la cual podemos entenderla como 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 así 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. (Carranza, 2021)

Teniendo un método seguro en el que realizar la oferta, se buscó que los licitadores se comunicasen con la administración pública mediante certificadores digitales que corroborase su identidad, entrando aquí la «Identidad soberana digital» (que veremos con mayor detalle veremos en el apartado siguiente). Con ello esencialmente se consiguió que se llevase acabo el registro y valoración de las ofertas que no precisasen juicio de valor alguno, siendo la Blockchain el intermediario y prescindiendo por ende de la mesa de contratación.

En lo que al proceso respecta, Carranza nos lo explica muy bien. El licitador se presentará a la oferta de la licitación generando una huella electrónica mediante Blockchain, la cual se presentaría y acreditaría mediante la función de *hash* que ya hemos abordado para una mayor seguridad. Con la finalización de las ofertas se pondría en relación las huellas y la función *hash* correspondiente a su presentación para su consecuente evaluación. En caso de no precisarse, siendo que la licitación es totalmente objetiva, entonces podríamos usar un *Smart Contract* guiado por la fórmula matemática por la que se seleccione dicha licitación. Llegó incluso a incorporarse la figura del gestor para su supervisión y un portal de acceso al público en el que podría revisarse la *Blockchain* donde el licitador no solo registra su *hash* sino que revisa las transacciones realizadas, dándose la transparencia requerida.

Con el fin de que se pudiese diferenciar las distintas licitaciones sin que hubiese ningún favoritismo, entra la identidad soberana digital, permitiendo una interacción totalmente segura y reconocible de ser totalmente necesario.

IV. LA IDENTIDAD SOBERANA DIGITAL

1. CONCEPTO BASE

Tras haber visto cómo funciona la tecnología Blockchain a partir de los distintos fragmentos de tecnología que la componen, el marco legal actual con sus impedimentos y posibilidades, así como el antecedente de Aragón en un caso sumamente practico, ahondaremos mas en la cuestión de la identidad soberana no como un medio si no un fin en sí misma.

En ella como ya hemos visto se da el uso de la Huella Digital. De esta cabe extender el uso que se le ha dado con la llamada *Self-Governance Identity (SSI)* O «Identidad soberana Digital".

Para entender lo que es la identidad soberana digital, es relevante conocer cuál es el fin de la misma. Esta comparte el principio básico de la identidad digital, entendiéndola como la información procesada por sistemas informáticos que permiten la identificación de una persona física o jurídica externa a esta. Si bien el concepto puede parecer muy extranjero, es más bien todo lo contrario pues nos referimos a los usuarios y contraseña que usamos para identificarnos en sitios web como *Facebook*, *Google* o *Hotmail* entre otros. La principal diferencia es que estos datos de identificación se encuentran guardados en las bases centrales de las respectivas organizaciones que sustentan los organismos mediante los cuales usamos

esa identidad. En ocasiones habremos tenido la oportunidad de acceder a distintos medios y plataforma únicamente con esta identidad «Accede/identifícate con tu cuenta de *Google*/*Facebook*/*Hotmail*» para ahorrar tiempo y esfuerzo. En el momento en el que somos capaces de realizar dicho cruce de plataformas, hablaremos de una identidad federada.

El quid de la cuestión reside en que, si bien esos datos nos corresponden, figurando tras esa contraseña y usuario nuestro correo, nombres y más información. Los ecosistemas terceros a los que accedamos con esta identificación sabrán más de lo que precisan pues en ocasiones no podemos elegir qué información compartir y que no, dejándonos en un «todo o nada». Tampoco sabemos en especial en qué lugar se encuentran nuestros datos, o incluso cuantas entidades las poseen pues sin darnos cuenta muchas veces permitimos el compartir dichos datos con el fin de un contenido más «personalizado». En definitiva, poseemos nuestros datos, pero no nos pertenecen. (Entrando aquí la relevancia de leyes como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.)

Esta es la función que pretende llenar la identidad soberana digital, el ciudadano tiene tantos los medios para generar como para controlar y guardar (en su dispositivo propio) los identificadores únicos que le representan sin la necesidad de solicitar autorización/verificación a una entidad centralizada. (Comisión Europea, 2019) Desvinculando efectivamente nuestros datos personales de los ecosistemas creados por estas organizaciones (*Google*, *Facebook*...), permitiéndonos usar nuestros datos con total libertad, independencia y más importante, control.

La forma mediante la cual obtendremos total control de nuestros datos es precisamente prescindiendo del intermediario centralizado, y es en este punto en el que entra la *Blockchain*. Esta será el medio a través del cual se verifican dichos datos por el método de consenso, proporcionando así la seguridad que de otra manera terceros no tendrían entre sí. Sumando a esta su alta inmutabilidad y seguridad, tenemos un proceso automatizado a través del cual no solo verificar nuestros datos si no también elegir en qué nivel y grado los compartimos.

De forma un poco más concreta y utilizando las tecnologías ya explicadas, el papel que jugaría la *Blockchain* es pertinente en lo que se refiere a la creación de una identidad exclusiva a la persona a través del uso de la criptografía asimétrica. Mediante la función del *hash* criptográfico es posible la creación de una estampa temporal para la verificación de

autenticidad de dicha información en tanto que jugaría la inmutabilidad de la *Blockchain*. A dicho Hash se le proporciona una identidad, dicha identidad será la que se nos solicite por parte de un tercero para verificar por ejemplo nuestra edad. Mediante una *API* y un portal de acceso, en un proceso automatizado (*Smart contract)* este tercero puede conectar con el portal público que enlaza a la *Blockchain*, solicitando un dato concreto relacionado con dicha identidad. El resultado arrojado por el portal de la AP será «positivo» o «negativo» respecto a la petición del tercero, como puede ser para saber si somos mayores de edad para acceder a cierto contenido o si realmente poseemos cierto certificado. De la misma podrá quedar registrado en la misma *Blockchain* el acceso que demos a una compañía y a que parte de la información, permitiendo esa interoperabilidad entre plataformas tanto privadas como públicas. En última instancia y en un plano donde esta tecnología se implementa totalmente, sería posible incluso la configuración de *Smart Contracts* con los que dar acceso de forma limitada y efectivamente cortar acceso una vez se termina el tiempo de la forma en la que se ha programado. Una gran utilidad a esta aplicación la encontramos en el reciente borrador de Anteproyecto de Ley por el que se regulan los mecanismos aleatorios de recompensa asociados a productos de software interactivo de ocio publicado por el ministerio de consumo con el fin de regular las *lootboxes*, mecanismos semejantes a los juegos de azar y apuestas incorporados en los videojuegos que afectan a los menores. La solución actual la estipula en el artículo 6 de dicho borrador, por el que se precisará de una identificación documental como es el DNI. ¿Por qué dar mas datos sensibles a terceros conociendo los peligros en una era que se digitaliza más y más?

Por lo tanto, obtendríamos un medio a través del cual dar al ciudadano un control total de su información y gestión de la misma. Reduciendo considerablemente no solo la burocracia si no la inseguridad mediante una forma de interoperabilidad más robusta y personalizada. Si bien este es un funcionamiento básico, no es el único al que puede sujetarse pues debido al carácter mutable de esta tecnología, es posible prepararla para mayores usos a medida que se desarrolla e implementa.

2. EBSI

El uso de la *Blockchain* en la administración pública no es algo que quede para el entusiasmo de pocos. En Europa es muestra de ello la Resolución del Parlamento Europeo, de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación, concretamente en su ordinal 77: «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» (Carranza, 2021)

Con dicho reglamento, acompañado de la mano del reglamento eIDAS anteriormente mencionado, ya se han visto el primer proyecto con su fase de prueba encaminado a crear una Blockchain europea que pueda interactuar tanto el ciudadano como con empresas.

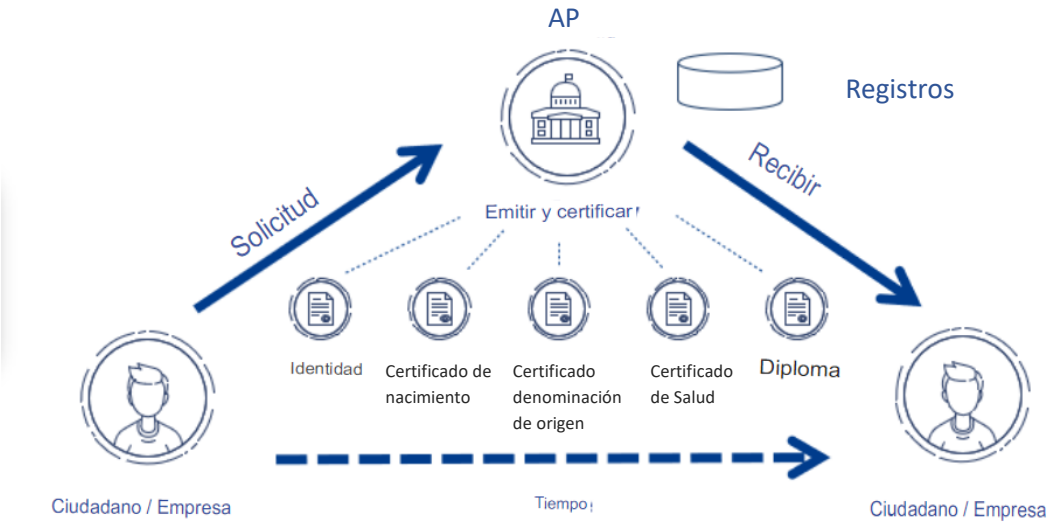


Fig. nº4 (Comisión Europea, 2020)

Este proyecto es conocido como *EBSI (European Blockchain Services Infraestructure)*. El objetivo de este es crear un estándar europeo mediante el cual poder interactuar de la misma forma en la que se establecen los estándares electrónicos en el reglamento eIDAS al igual que acelerar la creación de servicios internacionales para las administraciones públicas con el fin de verificación de la información. Esta *Blockchain* utiliza la criptografía asimétrica y las demás tecnologías de la misma forma en la que se ha explicado para la AIS.

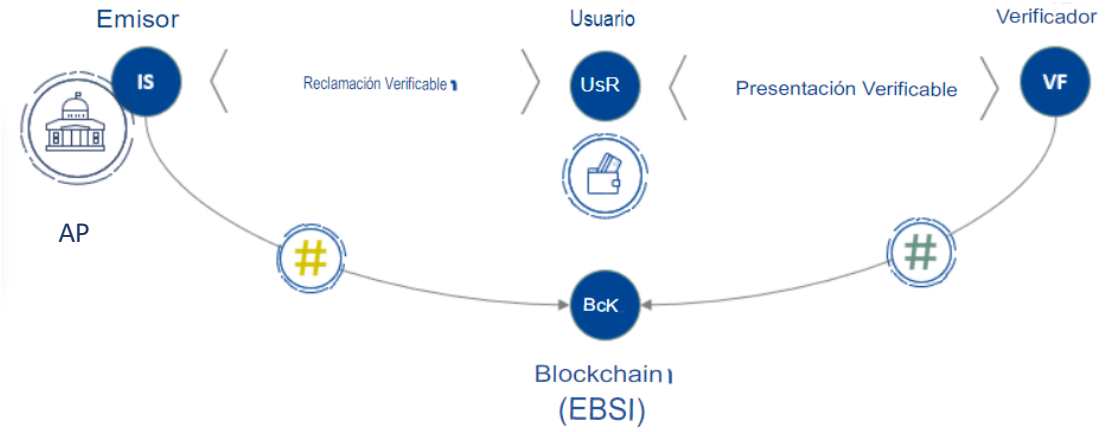


Fig. nº5 (Comisión Europea, 2020)

Por el momento se trabaja en que esta red pueda soportar no solo la identidad soberana digital, sino también la gestión de títulos universitarios, una forma segura a través de a cuál compartir datos, para la gestión de las peticiones de asilo, así como una red de comunicación para evitar el fraude. Como es comprensible, esta red de Blockchain busca expandirse por toda la unión europea, dando interoperabilidad con *Blockchains* tanto públicas como privadas. Es por esto que tomar esta como ejemplo no solo técnico sino regulatorio no solo es un «lujo» de innovación, sino una necesidad ante la que nos estaremos adelantando. Así pues, el enfoque a largo plazo que este proyecto tendría se dirige a poder complementar y operar en un futuro con la red *EBSI* en todos sus niveles.

En tanto que técnicamente el proyecto presentado y la *EBSI* son hermanas, no es de extrañar que legalmente también lo sean. Si bien ya se han llevado diferentes informes marcando el marco regulatorio de esta, la mayoría se han dado en virtud del reglamento eIDAS donde se acentúa como encajarán las distintas firmas, identificadores y certificados digitales. El segundo análisis que se busca realizar está relacionado con la protección de datos, actualmente se está elaborando dicho análisis. A continuación, veremos las cuestiones que considero de mayor relevancia y que la administración pública deberá tener en cuenta respecto teniendo al requisito que se nos solicita por parte del artículo 46.2 de la Ley 40/2015.

V. CUESTIÓN EN MATERIA DE PROTECCIÓN DE DATOS

1. ANÓNIMO O SEUDOANONIMO

Si bien en un apartado anterior hemos repasado el marco legal español sobre el que podría situarse la *Blockchain* en lo que a procedimiento administrativo y su régimen respecta, con el concepto de la identidad soberana digital y el requisito dado por el artículo 46.2 de la Ley 40/2015, ahondaremos en la ley reguladora de protección de datos. Sin embargo, no nos quedaremos en el marco español, sino que como ya habíamos visto en el artículo 3.3 del Real Decreto-Ley 14/2019, de 31 de octubre a través del cual se añadía la disposición adicional sexta de la Ley 39/2015 PAC nos encontramos con la oposición frontal a cualquier sistema de identificación basado en Blockchain… «[…] en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.»

Es por esto que, una vez presentada la idea principal, es de mayor relevancia una relación de esta tecnología con el marco europeo, que en el estrictamente español como el realizado anteriormente, en tanto que nuestra ley de protección de datos es a grandes rasgos una transposición de esta misma.

Así pues, nos encontramos con el reglamento (UE) 2016/679 del parlamento europeo y del consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)

Desde una perspectiva europea y más en lo que a protección de datos se refiere, no se entiende que pueda existir una *Blockchain* que se adapte o sea ideal a los requisitos y obligaciones que han de respetarse dentro del reglamento, si no que depende predominantemente del uso concreto que se le dé a esa Blockchain. Esto es así en tanto que no es sobre el sistema si no en como el sistema protege y **utiliza** esa información, buscando que esto lo haga de una manera en la que efectivamente se protejan nuestros derechos y se cumplan las obligaciones.

Este es un incentivo más por el que ver, desde una perspectiva legal el porqué es necesaria la adopción de esta tecnología en la administración pública, siendo el gobierno quien, aprovechando la mutabilidad de esta tecnología, moldee su uso en uno que respete los principios por los que se rige la administración. Debido a las necesidades que acarrea la administración pública, el tipo de *Blockchain* que más se acomodaría es aquella hibrida o

pública permisionada. Siendo estas las más populares y con las que existe una inmensa interoperabilidad, convirtiéndose en su vez la más prolifera a adaptarse al RGPD. (Tom Lyons, 2018).

Otro aspecto de extrema relevancia es el ver si los datos procesados a través de la Blockchain siguen cayendo enteramente bajo el alcance del RGPD. Como ya sabemos los datos que se procesan dentro de esta *Blockchain* sería mediando el uso no solo de la función de *hash* criptográfico sino también la criptografía asimétrica. Esto nos lleva a un punto en el que si bien los datos protegidos si son inherentemente parte del alcance del RGPD (como se sitúa en su artículo 2.1 y 4.1, poniendo como punto clave de dato personal la identificabilidad de los mismos) en el momento en el que estos datos se "anonimizan", el cómo utilicemos esos datos anónimos cae fuera del ámbito de aplicación del RGPD. (Grupo de Trabajo Nº216, 2014), así mismo lo vemos en el considerando 26 de la misma ley.

«Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. **Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios**, **como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física**. **Para determinar si existe una probabilidad razonable** de que se utilicen medios para identificar a una persona física, **deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación**, **teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima**, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. **En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima**, inclusive con fines estadísticos o de investigación.»

Recordemos que la inmutabilidad de los datos reside en parte en esa criptografía asimétrica y el hecho de que **solo** nosotros tenemos un acceso a esta, además de que esta se identifica no por nuestra identidad per sé, si no mediante el *hash* (el cual no es más que un código

alfanumérico a la vista). Es por eso que podríamos entender que la forma en la que se llegarían a tratar los datos personales en la Blockchain es anónima, lo cual de ser así caería fuera del ámbito regulatorio creando una cierta inseguridad jurídica a largo plazo.

Cabe matizar como de forma acertada se matiza en la Opinión 05/2014 del grupo de trabajo 216 (0829/14/EN WP216, P8), la información de carácter «identificada o identificable» dentro de este contexto se concluye que puede entenderse como datos anonimizados aquellos que previamente identificaban a una persona, siendo dicha identificación imposible en la actualidad. Así pues, comprendiendo la dificultad implicada en un método «imposible», la comisión entiende como suficientemente robusto un sistema donde las posibilidades de identificar al individuo sean «**razonablemente**» imposible

Sin embargo, hay problemas que considerar con esta información «totalmente» anónima, no por un problema actual en la tecnología o su incapacidad para protegerla y hacerla anónima como ya hemos visto. Si no porque la anonimización no debería ser tenida como un ejercicio de ejecución única, si no que necesita de una investigación constante a la par que nuevas tecnologías y las formas de usarla se dan.

En la actualidad, poniendo el énfasis en ataques de fuerza bruta, con un hash como el SHA-512 anteriormente expuesto, un dispositivo podría tomar mucho más de 100 años dependiendo del poder computacional y *bytes* de lo encriptado (Martin Bosslet, 2018). Sin embargo, como ya hemos dicho, la tecnología evoluciona rápidamente y la garantía en este método de encriptado corre contra el tiempo. Mientras nuestra clave pública resida en un lugar de la red, no es inconcebible pensar que eventualmente se consiga averiguar un método de romper estos algoritmos como ya ha pasado con otros de familias pasadas. Teniendo en cuenta la inmadurez de esta tecnología considero que la amenaza de una exposición a futuro es los suficientemente grande como para considerar la información seudoanonima, más que anónima. Esa capacidad de identificabilidad futura es lo que podría hacer que se clasificase como seudoanonimo, cayendo dentro del régimen del RGPD.

Otro de estos problemas es que de conocer partes de la información que se contiene no es inconcebible que un ataque de fuerza bruta como el expuesto anteriormente pudiese tener éxito) (Grupo de Trabajo Nº216, 2014).

En esencia, sería fácil cerrar aquí el debate y concluir pues que podremos regir esta nueva tecnología bajo el RGPD, pero por desgracia el debate sobre como considerarla se encuentra

aún sobre la mesa, principalmente porque la clave de la cuestión reside en los aspectos más técnicos. Hemos visto cómo con y por la tecnología actual es posible considerarla anónima y bien protegida, cumpliendo con el requisito de no reversibilidad ni riesgo de relacionar el *hash* con una persona, hay bastante incertidumbre sobre el «hasta cuándo». Su clasificación es precisamente muy difícil porque para cada uno de los problemas presentados existen formas de lidiar con ellos hasta un grado de seguridad, pero esto depende mucho más de la infraestructura técnica y legal con la que se dote más que la tecnología en sí. (Tom Lyons, 2018)

Esto nos deja una vez más en una posición que ya hemos visto anteriormente. No solo precisamos que sea la administración la que lleve la delantera en esta implementación, sino que necesitamos una legislación que regule esta materia de una manera efectiva, precisamente donde el RGPD podría no llegar.

Perfecto sería que no se diese ningún tipo de confrontamiento o «roce» con la normativa europea, pero raramente en derecho todo encaja a la primera (si es que alguna vez lo hace). Lo que hace especial los confrontamientos que pueden darse, es que depende enteramente de nosotros. Hemos visto que no depende tanto del concepto de *Blockchain* si no de la funcionalidad con la que dotemos y el tipo que usemos. Y es que los principios de funcionamiento son próximos a los del RGPD («licitud, transparencia, fines concretos, pertinencia, limitado, configurable para el tiempo en el que se precise y tratamiento seguro»– Art.1) en tanto que la solución que nos proporciona la *Blockchain* son los beneficios y seguridad de un tercero centralizado, como ha sido hasta ahora, pero automatizado. En este aspecto respecto al RGPD, la entidad responsable será aquella(s) creadora de la misma (en tanto esta sea permisionada o privada), dándose por responsable al gobierno de España, claro es si fuese este el primero en dar el paso hacia una identidad unificada, pasos ya recorridos por parte del sector privado como ya hemos visto (*Google, Facebook…*). En pocas palabras, no solo sería mucho más fácil su adaptación a la normativa europea, si no que trataríamos de forma personal con la seguridad ciudadana, teniendo la certeza de que es precisamente el interés público el que prevalece sobre cualquier interés privado que pudiese haber de licitar esta tarea en tanto que «ya tiene un ecosistema y mayor experiencia». Sería sin duda la forma más sensata de lidiar con las responsabilidades inherentes y legales de la infraestructura.

2. CUMPLIMIENTO DE LAS OBLIGACIONES

Es igualmente importante notar la forma en la que la administración podrá cumplir con los distintos derechos que encarna la protección de datos y suponen en cierto grado una dificultad para la *Blockchain*. (Artículos 15 a 22 Reglamento (UE) 2016/679).

Para poder proseguir con los consecuentes derechos, es importante notar que, debido a la naturaleza descentralizada de la *Blockchain,* puede hacerse difícil saber quién controla la *Blockchain,* o en todo caso a quién acudiremos a pedir responsabilidades si no hay un organismo claro. La siguiente relación de derecho-*Blockchain* se hace entendiendo que esta es de carácter confederada/pública permisionada bajo el control de la administración pública.

El derecho al acceso. Entendido como la posibilidad de saber si nuestra información se encuentra en posesión de un tercero, el propósito, distribución de esta, tiempo de guardado… El problema que supone el respeto de este derecho descansa precisamente en la incertidumbre de conocer el responsable tras la *Blockchain.* Siendo este la administración pública, uno único, se ve mayormente resuelta, pues siendo un único controlador con distintos nodos, siempre podremos tener ese «acceso» solicitándolo al único responsable.

El derecho de rectificación y al olvido es quizá sean los más problemáticos para la *Blockchain* debido a la forma en la que esta funciona (recordemos su inmutabilidad para garantizar confianza y seguridad). Una vez más, la solución a este problema reside principalmente en quien se encuentra en control de la *Blockchain* y que acción podrá tomar. Teniendo la cuestión principal solucionada (pues es la administración pública), la secundaría será ¿cómo vamos contra la propia naturaleza de la Blockchain? En mi opinión, no tenemos por qué. Dependiendo del método de encriptado que usemos, como es el expuesto en este caso con la existencia de una clave pública y privada, sería posible considerar legalmente el "borrado" a través de eliminar completamente la clave privada con la que conseguir acceso (Comisión Nacional Informatica y de Libertades, 2018). De la misma manera podríamos atajar el problema de la rectificación, mediante la destrucción de la clave perteneciente a los datos puestos y su reconstrucción con la generación de un nuevo juego de claves.

El derecho a la limitación del tratamiento, con la idea en mente de la identidad soberana, entiendo que es un derecho que se cumple «por defecto». Nos encontramos con que el único organismo que conocerá de esta información será la administración pública, quien por necesidad necesita de esta igualmente. La forma en la que se podrá interactuar con terceros

no tiene por qué precisar el compartirla como hemos visto anteriormente, siendo este en mi opinión el punto fuerte de esta.

El derecho de oposición, una vez más este es un problema que tiene una relativa fácil solución cuando es la administración pública quien está a cargo de esta. Debido al funcionamiento propuesto, la forma en la que serán tratadas los datos dependerá mayormente del ciudadano, siendo este el punto de una identidad soberana. El Estado será fundamentalmente quien «guarde» dicha información para que el ciudadano la use, no teniendo intereses más allá del público.

Respecto al tratamiento automatizado de datos, el derecho a no ser objeto de una decisión por un acto automatizado, así como elaboración de perfiles, podría verse afectado en tanto al uso que le demos a la *Blockchain*. Inherentemente y exclusivamente a rasgos de la identidad soberana de la forma expuesta anteriormente, ningún perfil ni decisión debería realizarse, entiendo claro está que sea la administración pública quien este a cargo de este.

En resumen y en total acorde con lo expuesto, así como con el artículo 25 RGPD, la protección de datos desde el diseño y por defecto ha de ser el aspecto clave de la Identidad soberana y su *Blockchain*. Resaltando lo dicho, la mutabilidad de la Blockchain puede ser la clave para una implementación acorde al derecho, siendo este el que moldee la Blockchain y no viceversa.

VI. CONCLUSIÓN

Si bien la aplicación a la que más se ha hecho hincapié en este escrito ha sido en torno a la identidad soberana digital, es importante no olvidar que la implementación presentada es solo la base de esta. Pues hablamos de una infraestructura pública que no solo cambiaria la forma en la que nos comunicamos con el sector público, sino también con el privado. Siendo una posible herramienta que sirva para asegurar los aspectos materiales más intangibles de nuestra actualidad como es el internet. Permitiendo así ampliar la cartera del ciudadano en una que más allá de su identidad, permita certificar sus propiedades y validarlas frente a terceros, restringir el uso a los menores a ciertos lugares de la web, y más importante, ser capaces de hacer cargar con la responsabilidad a los usuarios de la web sin necesidad de faltar al anonimato que caracteriza el internet, entre muchas otras…

Cierto es que no existe en la actualidad un marco perfecto, o idóneo en el cual encajar esta nueva forma de interactuar con la administración, como ya hemos visto no hay barreras inexpugnables que de igual manera impidan su aplicación y futura implementación. Este tipo de tecnologías son las que llevan no a una digitalización de la administración, pasando los mismos tramites existentes por un escáner, si no que realmente crean todo un ámbito tecnológico en la que esta se mueve y desarrolla independiente pero no al descompás de su contraparte física.

Considero ante todo que no debemos avanzar por avanzar, implementando cualquier novedad tecnología, siendo por ello necesario una legislación temprana que no solo garantice los derechos de los ciudadanos, sino que permita una evolución continuada compenetrada con los principios por los que se rige la AP. No podemos dejar de lado tampoco el hecho de que estas tecnologías ya se han implementado en una menor escala dentro del territorio europeo, entendiéndola como inevitable, es preciso y casi obligatorio a mi parecer que por primera vez demos el paso hacia delante. Hacia una administración electrónica más económica, eficiente, segura y actual que sea capaz de conectar con la ciudadanía de tú a tú.

BIBLIOGRAFÍA

Aerts, N. K. (2011). *Cryptanalysis of hash functions.* Eindhoven: Eindhoven University of Technology.

Arshdeep Bahga, V. K. (2016). *Blockchain Platform for Industrial Internet of Things.* Atlanta, GA, USA: Scientific Research Publishing Inc.

Baldegger Rico, P. S. (2019). *THE CRYPTO ENCYCLOPEDIA Coins, Tokens and Digital Assets from A to Z.* Switzerland: GROWTH.

Branstad, D. K. (1983). *Report of the Nist Workshop on Digital Signature Certificate anagement.*

Brown, K. (2013). *The Dangers of Weak Hashes.* GIAC directory of certified professionals.

Carranza, J. C. (2021). Adjudicación de contratos públicos mediante Blockchain. *Wolters Kluwer*, 4-5.

Finck, M. (2019). Blockchain Regulation and Governance in Europe. In M. Finck, *Blockchain Regulation and Governance in Europe* (p. 33). Cambridge University.

Halil Saltik, S. A. (2022). *Secure Hash Algorithm - 512 In Blockchain.* Düzce, TURKEY: Department of Software Development.

Martin Bosslet, M. B. (2018). *StackOverflow*. Recuperado el 06/12/2022, de StackOverflow: https://stackoverflow.com/users/827060/emboss

Szabo, N. (1997, Septiembre 1). Formalizing and Securing Relationships on Public Networks. *First Monday, 2*(9).

Tom Lyons, L. C. (2018). *BLOCKCHAIN AND THE GDPR.* European Commission.

OTROS DOCUMENTOS CONSULTADOS

Comisión Europea . (2010). *The European eGovernment Action Plan 2011-2015.* Brussels.

Comisión Europea. (2019). *eIDAS supported self-sovereign identity.*

Comisión Europea. (2020). Retrieved from EBSI: https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=381517902

Comisión Nacional Informatica y de Libertades. (2018). *Premiers éléments d'analyse de la CNIL.*

UK Government Chief Scientific Adviser. (2016). *Distributed Ledger Technology: Beyond Blockchain.*

Grupo de Trabajo Nº216. (2014). *Opinion 05/2014 on Anonymisation Techniques.* Brussels: European Commission.