Las aplicaciones del *Blockchain* a las actividades de las fundaciones y a sus relaciones con la Administración Pública

Efrén Díaz Díaz
Abogado
Asociado Senior del Bufete Mas y Calvet
Especialista en Derecho Administrativo y Geoespacial

Fernando Moreno Cea
Abogado
Miembro del Consejo Asesor de la Asociación Española de Fundaciones

I. Introducción

El estudio que a continuación se presenta surge como resultado del interés mostrado desde la Asociación Española de Fundaciones por la aplicación práctica de la nueva tecnología del *Blockchain* a los ámbitos, tanto privados

como públicos, en los que habitualmente se desarrollan las actividades de las fundaciones. Muestra de ello son los diversos artículos que han ido apareciendo en sus publicaciones y boletines, así como su introducción en los temas a tratar en cursos, seminarios, etc., por ella organizados. Todo este material ha constituido, sin duda, un punto de referencia en el análisis que en este trabajo se presenta de manera abierta.

Por otro lado, diversas entidades han sido ya pioneras en la utilización de esta técnica en sus propias actividades, lo que nos permite poder evaluar sus posibilidades de éxito actuales. De todas formas, queda aún mucho camino por recorrer. En este sentido, será preciso acabar de perfilar su aplicación a campos tan diversos como el control de los donativos recibidos por las fundaciones, asegurar que las ayudas que conceden son destinadas realmente al fin perseguido, la gestión de datos de colectivos de personas en sus actuaciones relacionadas con grandes catástrofes, la ejecución de proyectos en colaboración con otras entidades respecto de los que cada una de las intervinientes aporta diferentes medios humanos y materiales, y muchos otros similares que la práctica pueda mostrar como idóneos para la aplicación del *Blockchain*.

Asunto distinto es la posible aplicación de esta tecnología a las relaciones con la Administración Pública; en concreto, ya que nos estamos refiriendo a las fundaciones, las relaciones con el Registro de Fundaciones y el Protectorado. Tal y como en este estudio se indica, sería fácil arbitrar protocolos para la realización de actos que podríamos calificar como de «materiales». Serían aquellos que tuviesen como fin la aportación de documentos que contuviesen datos cuya recepción no supusiese la intervención de un funcionario que tuviese que calificarlos o bien acceder a una solicitud presentada por una fundación. Está claro que en estos casos no bastaría con el desarrollo actual de esta tecnología, la cual además necesitaría para su aplicación la necesaria base legal, por ahora inexistente en nuestro país, aunque ya hay algunos, como por ejemplo Malta, que han comenzado a legislar sobre la materia.

Finalmente, la aplicación del *Blockchain* suscita el grave problema, que por sí solo podría ser el objeto de un estudio específico, de su adecuación a la normativa sobre protección de datos personales. Piénsese, por ejemplo, en la dificultad de poder recabar la aceptación formal e inequívoca de la inclusión de los datos de personas afectadas por un terremoto y cuya gestión se desea efectuar con la aplicación de esta tecnología. O en cómo eliminar los datos de las personas que, en el ejercicio del derecho que la legislación europea vigente les reconoce, así lo solicitan. Es sin duda este un campo totalmente abierto al estudio y realización de aportaciones que puedan ser introducidas en futuras modificaciones de la actual normativa.

Esperamos que esta colaboración anime a las personas y entidades que realizan actividades a las que puede ser de aplicación la tecnología del *Blockchain*, a continuar con sus esfuerzos por hacer que esta pueda ser dentro de unos años un instrumento tan ordinario y asequible al público en general como lo es hoy en día Internet.

II. *Bitcoin*, *Blockchain* y algunos conceptos

Blockchain, o la tecnología de «cadena de bloques», es la infraestructura de las novedosas criptomonedas, incluida el «Bitcoin».

El *Blockchain* crea una cadena digital de registros con enlaces encadenados para formar un registro inmutable, único e irrepetible. Cada bloque de datos se eslabona al anterior para completar la cadena. Se consigue así un registro distribuido, resistente a la sincronización, es decir, inmutable y permanente. Resulta útil para controlar la seguridad de la información, a través de protocolos para verificar y proteger las innumerables operaciones que se producen en su entorno. Se trata de una base de datos que no permite borrar o modificar, sólo posibilita escritura bajo consenso. La forma de archivo y la seguridad que proporciona técnicamente *Blockchain* permite comprobar si el documento generado ha sido alterado en algún momento posterior al registro.

Esta cualidad del *Blockchain* en el entorno financiero ha supuesto una ventaja, pues aumenta la transparencia y evita el doble gasto de divisa, mediante la descentralización de pagos electrónicos. Sin embargo, la cadena de bloques tiene nuevas aplicaciones, que no se limitan a criptodivisas y van mucho más allá, si bien esa característica de inmutabilidad plantea serios inconvenientes. Por ejemplo, en la creación de contratos inteligentes (*Smart Contracts*) con almacenamiento de documentos y en el Internet de las Cosas (*Internet of Things*), incluidos los registros públicos y administrativos, todo ello entendido como plataforma de dispositivos y máquinas digitales interconectados entre sí, sin necesidad de contacto directo con los seres humanos.

El *Blockchain* aún está en un estadio inicial de desarrollo y ciertamente no existe una regulación sectorial específica para esta tecnología de última generación. Como *Bitcoin* ha sido el principal usuario de esta infraestructura, el debate regulatorio se ha focalizado en esta materia, más financiera y monetaria. Pero sus aplicaciones multipropósito comportan vacíos legales que abarcan desde armonizar la fiscalidad de las transacciones hasta la prevención de su uso para fines ilícitos, pasando por el régimen jurídico aplicable a los registros públicos exigidos por disposición legal, como los administrativos, mercantiles, de la propiedad de inmuebles e intelectual.

III. *Blockchain* y su funcionamiento

1. *Descripción general de la operativa del* Blockchain

Blockchain es un sistema revolucionario que, fundamentalmente, provocará la desaparición de muchas de las cosas repetitivas de la vida personal y profesional.

En la actualidad, y en el modo en que hemos conocido hasta ahora el funcionamiento del mundo, se necesita producir, gestionar y almacenar en todo momento una enorme cantidad de información certificada, en el sentido de validada por terceros de confianza. Cada día, cada hora, cada segundo, incontables actividades y operaciones requieren una confirmación o validación segura.

Hasta ahora esta gestión de certificación la han hecho los seres humanos, basados en la confianza mutua. No obstante, las personas pueden ser lentas, despistadas, corruptibles, perezosas o hedonistas. Por ello, la propuesta de *Blockchain* es que este trabajo pasen a hacerlo otra clase de seres, considerados *incorruptibles, eficaces, sacrificados y cada día más veloces.* Los ordenadores. Pero, como contrapunto, también es conocida la gran debilidad de un sistema informático: que es *hackeable*, atacable, destruible.

El *Blockchain* evita esta debilidad de los sistemas informáticos no con un superpoderoso antivirus ni con un vigoroso *firewall* o medidas electrónicas o digitales similares. *Blockchain* se autoprotege gracias a su propia estructura, su propia arquitectura. *Blockchain* significa *«cadena de bloques»*. Y se debe a que se trata de una sucesión conectada y vinculada de bloques que contienen información. Cada bloque puede contener diferentes tipos de información. Hasta la actualidad el ejemplo más conocido es el de la criptomoneda *Bitcoin*, pero existen muchos otros en proyectos de trazabilidad de productos y de prestación de servicios a personas, además de proyectos solidarios donde es fundamental asegurar el destino de los donativos realizados.

Para ofrecer una descripción más general que permita entender luego los diversos conceptos, cada bloque de esa cadena tiene tres cosas. La primera es la información. En el caso del *Bitcoin*, por ejemplo, contiene la información relativa a la transferencia de dinero: emisor, receptor, fecha, cantidad, etc. La segunda es algo muy importante: el «hash». El *hash* es el número de identificación del bloque. Se trata de un número único e irrepetible, de igual extensión con independencia del contenido. Cada uno de los bloques tiene el suyo propio. La tercera tiene el *hash* del bloque anterior.

Por tanto, cada bloque queda conectado con su predecesor y sucesor. Así se ve claro lo de «chain», cadena. Efectivamente, los bloques van creando una cadena, que es lo que define la estructura interna del *Blockchain*. Sin embargo, conviene saber por qué el *Blockchain* es *«inhackeable»*. En principio lo es por dos cuestiones unidas. La primera, por el *hash*. La segunda, porque muchas personas están observando a la vez y permanentemente. El *hash*, como hemos señalado, es el número único de cada bloque. Pero tiene una gran peculiaridad y es que el número se genera según el contenido del bloque. Eso significa que si se cambia el número del bloque, la información automáticamente cambia el *hash*. Se puede imaginar como una pieza de puzzle. Según la información tendrá una determinada forma. Si alguien cambia la información, la forma también cambiará por lo que dejará de encajar y la cadena quedará invalidada. No es que haya una única base de datos, sino que cada usuario de *Blockchain* tiene una «copia» de ella. Dado que muchas personas están observando de forma continuada, si un usuario altera la información de su copia, la comunidad lo sabe. Por lo que «su versión» de la base de datos queda invalidada y sin efecto. Ahí está la diferencia: la seguridad y la certificación de los documentos en *Blockchain* se la dan los usuarios. No una gran institución, no un banco, no un fedatario público, sino usuarios iguales pero en gran número.

La manera de *Blockchain* de conseguir estos objetivos se realiza con base en los dos motivos siguientes, pues son las dos razones principales por las que un usuario puede decidir unirse a la red. Simplemente para usar el sistema o bien para hacer algo mucho más goloso: crear nuevos «blocks» (bloques) para la «chain» (cadena). Se trata de los denominados en el argot como «mineros».

Muchos de los partícipes en el *Blockchain* no están allí para usar los servicios del sistema, sino que sólo quieren una cosa: crear nuevos bloques. Los llamados mineros, a medida que se van firmando contratos, haciendo transferencias o cualquier otra clase de valor añadido, asumen la necesidad de almacenar esa información en un nuevo bloque. Para añadir un nuevo bloque a la cadena hay que resolver un problema matemático muy complejo. Para resolverlos hace falta una gran potencia de computación, así que los mineros ponen sus procesadores al máximo rendimiento posible para intentar resolverlo en el menor tiempo posible. Una vez que consideran que lo han resuelto, el resto de la comunidad verifica que la solución es efectivamente acertada. Si lo fuera, un bloque nuevo se agrega a la cadena, la información queda consolidada y el acuerdo correspondiente se efectúa. Y lo más importante es que el minero que ha encontrado la clave cobra la recompensa. En el caso de *Bitcoin*, esa recompensa alcanza los 12,5 *bitcoins*. Es una suma considerable si se considera que actualmente cada *bitcoin* vale aproximadamente 10.500 dólares americanos.

Sin embargo, *Blockchain* no siempre ha sido tan popular como hasta ahora. En sus comienzos prácticamente nadie le prestó atención. El sistema *Blockchain* fue creado en 1991 y no fue utilizado efectivamente hasta 2009 cuando Natoshi Nakamoto, de quien aún hoy se duda acerca de su verdadera identidad e incluso se piensa que se trata del pseudónimo de un grupo de informáticos, lo empleó como infraestructura para su ahora conocidísimo *Bitcoin*.

Pero *Blockchain* no es únicamente *Bitcoin* y es más que *Bitcoin*. Las aplicaciones efectivas de este sistema pueden ser muy diversas: desde firmar contratos inteligentes, ejercer el voto en elecciones, guardar registros médicos, bancarios y administrativos, y muchas otras utilidades que todavía están por descubrir. Por ejemplo, con *Blockchain* sería imposible falsear la procedencia de los alimentos o esconder si durante su transporte, se ha roto la «cadena de frío». De igual modo, en el ámbito de la salud sería imposible manipular los historiales médicos. En el comercio de joyas, el poder rastrear desde su origen hasta su compra permitiría al consumidor asegurarse de que no está comprando, por ejemplo, un «diamante de sangre». Se trata, en resumen, de almacenar información con muchas personas observando a modo de testigos, lo que dificulta que la información sea falseada.

En definitiva, *Blockchain* es mucho más que una simple base de datos, pues es un sistema de almacenamiento de información fuera del sistema convencional, una herramienta que busca crear una sociedad más equitativa, más transparente y más veraz.

2. *Aspectos de interés*

La existencia de un «Internet abierto y seguro» es una realidad irreversible, como reconocen desde las autoridades administrativas hasta los principales reguladores.

La diferencia que presenta el *Blockchain* es su acceso por consenso y un acceso restringido de los interesados. Esta propiedad se complementa con su alto grado de transparencia, pues el *Blockchain* es transparente gracias a la encriptación, que permite plena nitidez para los de dentro a la par que un encriptado para los de fuera.

El *Blockchain* comporta un esfuerzo de los protocolos digitales establecidos, una fuerte puja para ofrecer seguridad y estabilidad digital y entornos electrónicos de intercambio de información y, sobre todo, de bienes.

Una última propiedad relevante del *Blockchain* se cifra en su inmutabilidad, la cual debe ser analizada desde la óptica jurídica para extraer sus ventajas y,

en algunos casos, eventuales desventajas o conflictos de interés, como se analizará más adelante.

No hay duda de que nos encontramos ante una tecnología vanguardista de última generación, pero vinculada al mundo no lucrativo, en particular de fundaciones y asociaciones como ponen de manifiesto los actuales proyectos y principales usos dados. En este aspecto, con el *Blockchain* ocurre al contrario que con otras tecnologías. No comienza por el ámbito comercial o sólo empresarial, sino que se ha desplegado mayoritariamente en actividades y proyectos sin ánimo de lucro que requieren un alto grado de visibilidad y transparencia.

Con este enfoque, ya en los albores del *Blockchain* podemos afirmar, como se hiciera ante la aparición de Internet, que no parece que sea una cuestión que se presente simplemente de largo recorrido y pueda resultar muy importante. Por sus propiedades y características, más que de una tecnología innovadora, en la práctica realmente es y será una cultura. Una prueba elocuente de esta nueva realidad es la preocupación e interés técnico y jurídico que esta tecnología despierta de forma multisectorial.

Más en particular, múltiples sectores de la sociedad, la economía y la industria, además de la Administración Pública, guardan estrecha relación con el *blockchain*, precisamente con el fin de alcanzar un Internet seguro, lo que comportará una significativa contribución al desarrollo nacional y del entorno digital en su conjunto.

3. *Su funcionamiento*

A) *El* Blockchain *como tecnología*

La explicación y descripción del *Blockchain* como un herramienta o infraestructura tecnológica tiene una notable complejidad, por los elementos que integran el ecosistema digital. Por ello, seguidamente interesa conocer al menos someramente algunos aspectos que, siendo eminentemente técnicos, son la base para una mejor compresión de la naturaleza, objeto, alcance y propiedades de esta tecnología. En particular, porque podría tener un especial impacto en el entorno jurídico, tanto como soporte de actos y negocios jurídicos, como instrumento en las relaciones entre particulares y, sin duda, en las relaciones de los administrados con la Administración Pública competente.

Por el objeto de este estudio, ofreceremos una descripción sintética y progresiva, sin ánimo de exhaustividad y con el esperado fin de ayudar al

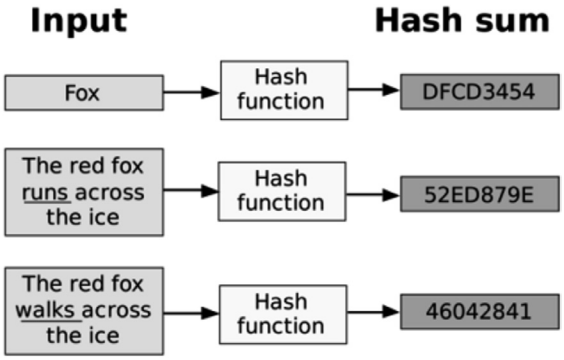
lector a comprender mejor los posteriores aspectos jurídicos que se asientan sobre los desarrollos tecnológicos del *blockchain*.

B) *Funciones* Hash

La función *Hash* es una de las bases del *blockchain*. Una función *hash* es una función unidireccional, pues convierte un dato de cualquier longitud en un resultado binario de longitud fija. Por tanto, el *hash* siempre es el mismo para el mismo valor de entrada, de manera que cualquier variación del dato original debe modificar el resultado del *hash*.

En la siguiente imagen se muestra conceptualmente la transformación de una información alfanumérica de cualquier extensión en un resultado binario de igual extensión.

Ejemplo de función *Hash*[1]



C) *Cifrado de clave pública y privada*

En relación con las funciones *Hash*, los cifrados asimétricos incluyen un par de claves. Explicado de forma sencilla, significa que si se cifra con una clave, únicamente se podrá descifrar con la otra clave y viceversa.

La clave privada es aquella que guarda el usuario y no se comparte con nadie. En cambio, la clave pública es la que el usuario hace pública para que todo el mundo tenga acceso a ella y pueda realizar las operaciones necesarias. Según el modo en que se utilicen ambas claves por el sistema, habrá múltiples casos de uso.

[1] Fuente: *https://brilliant.org/wiki/secure-hashing-algorithms/*.

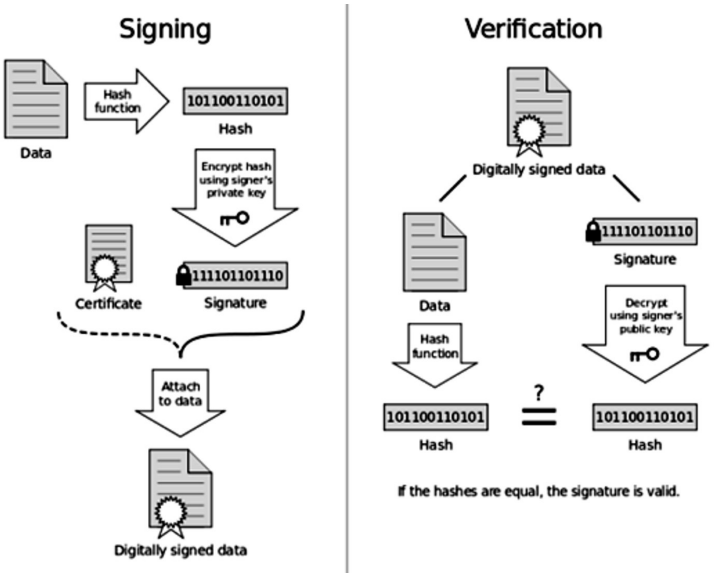
D) *Autenticación mediante firma digital*

La firma electrónica[2] se utiliza para autenticar un mensaje o documento. Para firmar se realizan tres pasos: primero, se crea un *Hash* del mensaje que se va a firmar, luego se encripta el *hash* con la clave privada del firmante y, finalmente, se envía el mensaje original junto con el *hash* encriptado.

Para comprobar la firma se siguen los tres siguientes procesos: primero, se desencripta el *hash* encriptado, seguidamente se crea de nuevo el *hash* del mensaje original y, al fin, se comprueba que los dos *hash* coinciden. Se obtiene así la comprobación de la identidad sin que se comprometa la seguridad ni se conozca la clave privada.

En la siguiente imagen se resume el proceso de firma y autenticación de la identidad.

Proceso de firma y autenticación de la identidad[3]



[2] Cfr. Ley 59/2003, de 19 de diciembre, de firma electrónica, Reglamento eIDAS UE 910/2014, Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

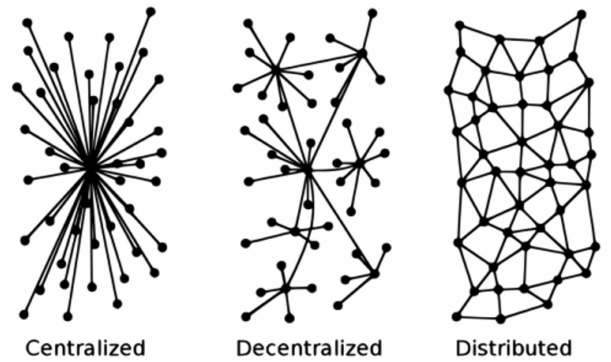
[3] Fuente: *https://stackoverflow.com/questions/46141265/how-does-the-verification-server-recognize-which-public-key-to-use-in-rsa.*

4. Blockchain *a vista de pájaro: ¿Qué es* Blockchain*?*

Blockchain es un conjunto de tecnologías, como antes se ha señalado. Lo interesante es que en su combinación hacen posible gestionar información compartiendo un registro.

Este registro se encuentra distribuido, descentralizado y sincronizado entre todos los nodos del *blockchain*, lo cual inviste a esta tecnología de una potente cualidad para su transparencia y utilización multinivel y multiusuario, pues se puede afirmar que *todos tienen todo*, al menos potencialmente y en cuanto a la posibilidad de verificación.

Clases de *Blockchain* según organización[4]



A) *Almacenamiento seguro e «inmutable»*

La información en *Blockchain* se transmite y se guarda de un modo extremadamente seguro y respeta la identidad, gracias al uso de claves criptográficas y firma digital. La información no puede ser alterada y además no se puede deshacer o reescribir información ya registrada. Cada cambio implica registrar nueva información. En consecuencia, todos los datos registrados son públicos y visibles para cualquiera que participe en la red.

B) *Descentralizado*

La organización del *Blockchain* es descentralizada, no existe un servidor o autoridad central. Por ello, se trata de un sistema de confianza «sin interme-

[4] Fuente: *https://steemit.com/blockchain/@crypto-talks/i-introduction-to-blockchain-treading-guide-1-familiarization.*

diarios» mediante «mecanismos de consenso», que posteriormente explicaremos.

En el *Blockchain* no cabe, *a priori*, posibilidad de fraude o doble gasto, precisamente por su configuración descentralizada. Todos los nodos tienen una réplica del último estado y además todos los nodos pueden verificar la información almacenada. Con este sistema se detecta cualquier intento de modificación fraudulenta y, lo que es más interesante jurídicamente, queda establecida la trazabilidad de todas las operaciones realizadas.

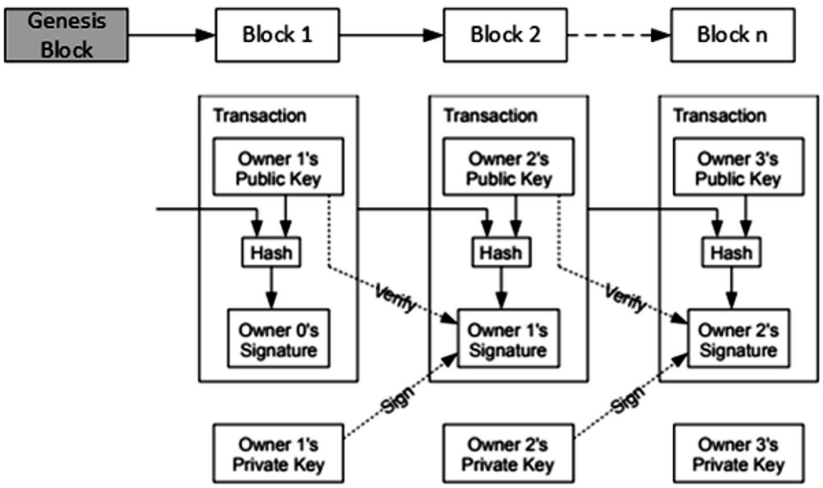
En consecuencia, se trata de un sistema que ofrece una alta resistencia a ataques informáticos y a prácticas fraudulentas.

C) *La «cadena de bloques»*

En el *Blockchain* los datos se almacenan en bloques. Cada bloque contiene múltiples transacciones. Cada bloque está ligado al bloque anterior. Los bloques están firmados y securizados mediante criptografía y la cadena contiene todos los datos y cambios desde su origen. También se le llama *distributed ledger* (*libro de contabilidad distribuido*)[5].

En la siguiente ilustración se muestra un ejemplo de «cadena de bloques».

Ejemplo de «cadena de bloques»[6]



[5] Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., … & Ellithorpe, M. (2016). Distributed ledger technology in payments, clearing, and settlement.

[6] Fuente: *https://jeevith20.wordpress.com/2017/07/03/mining-in-a-blockchain/*.

a) Contenido del *Blockchain*

El *Blockchain* contiene datos y transacciones. Una transacción es una operación sobre los datos.

Lo significativo es que estas transacciones pueden estar configuradas de la siguiente manera. En primer lugar, pueden estar predefinidas en el *Blockchain*, como por ejemplo en el caso del *Bitcoin*. En segundo término, pueden ser definibles por los usuarios, como ocurre en los *Smart Contracts*. Así, un *Smart Contracts* permite definir el concreto código que se ejecuta al realizar una transacción. Si el *Blockchain* soporta *Smart Contracts*, estos también se almacenan en el *blockchain*.

b) Trazabilidad y auditoria

El *Blockchain* lleva un registro estricto y detallado de todos los cambios que se han hecho sobre los datos. Los datos están replicados, pues todos los nodos contienen todo el historial completo de cambios.

Esta funcionalidad es muy útil para realizar tareas de auditoria, al ser posible comprobar cualquier operación desde el origen del *blockchain*. Esta trazabilidad se consigue gracias al enlazado de la cadena de bloques. Los llamados auditores pueden ser miembros del *Blockchain* y tener su copia siempre actualizada de los datos.

Se puede comprender mejor a través de un ejemplo como el de los «diamantes de sangre», pues el *Blockchain* se utiliza como registro para identificar cada diamante y poder seguir su trazabilidad desde el momento de su extracción. Las propiedades, características, descripciones y todo el ciclo de vida de movimiento del diamante y la transmisión de la titularidad de cada dueño, así como los fabricantes, minoristas y consumidores, queda registrado. Esta cualidad de registro ofrece seguridad jurídica y garantía de la legalidad de los cambios de propiedad.

Algunas empresas ya han desarrollado la tecnología del *Blockchain* movidas por el interés en el viaje de sus diamantes y joyas, así como por el deseo de la industria de demostrar autenticidad, transparencia y procedencia. El trabajo con un amplio conjunto de partes interesadas en toda la cadena de suministro de diamantes, desde los fabricantes de diamantes hasta los minoristas intermedios, ha propiciado que algunas entidades hayan cifrado la procedencia de más de 2 millones de diamantes en tres años.

En definitiva, ha sido posible debido a que las características principales de *blockchain* son inmutabilidad, velocidad y seguridad, y permiten crear la

plataforma adecuada para rastrear y proteger activos de alto valor y datos críticos. La naturaleza descentralizada de *Blockchain* proporciona seguridad para los registros. La información también se asegura a través de métodos criptográficos.

Una combinación de registros públicos y autorizados permite que todos los interesados tengan accesibilidad a la procedencia del diamante, pero también controla el acceso a información privada y confidencial exclusivamente para usuarios autorizados.

c) *Bitcoin* a vista de pájaro: ¿Que es *Bitcoin*?

Bitcoin es la base y el origen de todas las tecnologías de *Blockchain* del mercado. Es conocida por ser la primera tecnología de «dinero digital» de uso extendido. En este sentido, su popularidad se ha visto acrecentada porque se mantiene exclusivamente por la comunidad. Interesa su análisis porque facilita una mejor comprensión de otros posibles usos del *Blockchain* y porque en la actualidad constituye la plataforma más desarrollada.

La red de *bitcoin* permite realizar transacciones de dinero digital entre miembros de la red. La red es anónima y descentralizada, nadie tiene el control sobre ella, no hay regulador competente.

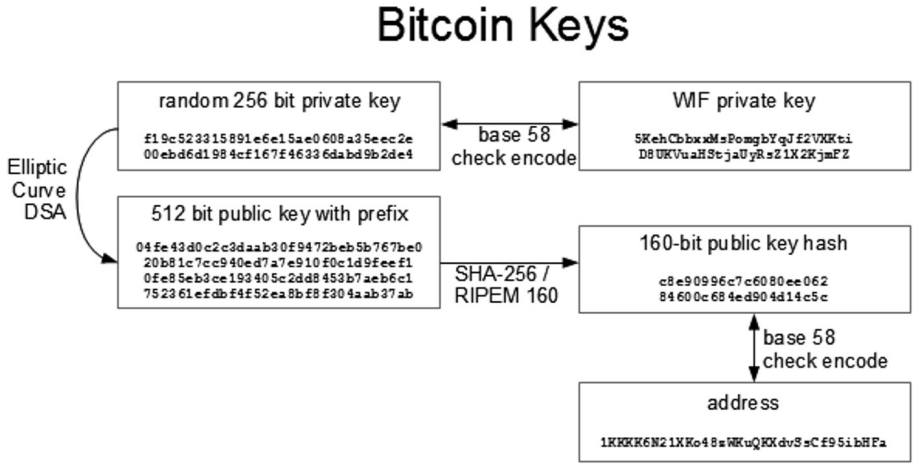
La seguridad se basa en criptografía y un mecanismo de «consenso» llamado «Prueba de trabajo» (*proof of work*).

d) Dirección y claves

Lo primero que se necesita para trabajar con *bitcoin* es una dirección (*address*) con la que crear una clave pública y privada, como antes se ha explicado. De este modo, la dirección es un «hash» de la clave pública. La dirección, por tanto, es la «clave pública», pero se utiliza el *hash* para que no sea tan larga.

En el supuesto de pérdida de clave, la clave privada se utiliza para firmar transacciones de dinero contenido en una dirección. Sin la clave privada es imposible transferir el dinero. Pero si se pierde la clave privada, cuyo descifrado es prácticamente imposible con los actuales sistemas computacionales, se pierde el dinero transferido o custodiado. No debe sorprender. Es como el «dinero físico», si lo perdemos no hay forma de recuperarlo.

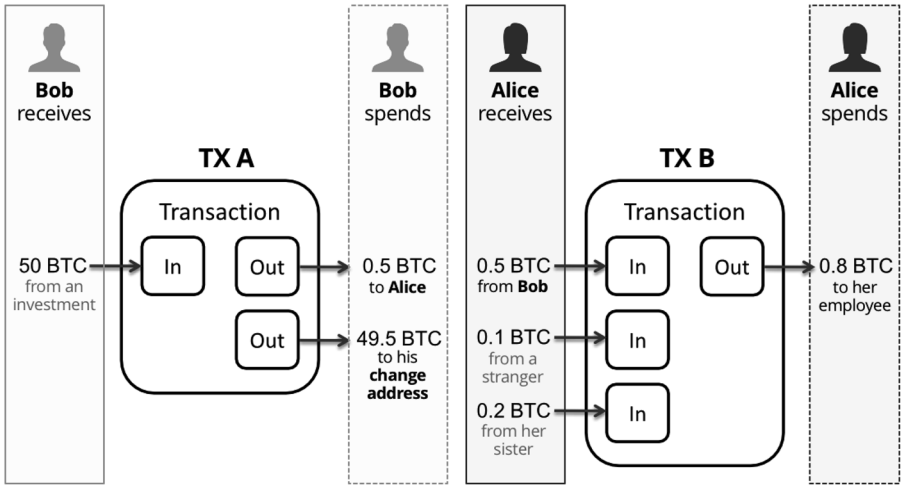
Ejemplo de clave y dirección de *Bitcoin*[7]



D) *¿Qué es una transacción?*

Una transacción es un intercambio de *bitcoins* de una dirección a otra. No existe el concepto de *«balance (saldo) por cuenta»*. Únicamente existen transacciones.

Ejemplo de transacción[8]



[7] Fuente: *https://crypto.stackexchange.com/questions/33821/how-to-deal-with-collisions-in-bitcoin-addresses*.

[8] Fuente: *https://freedomnode.com/guides/17/how-bitcoin-works*.

El origen de una nueva transacción, es una o más transacciones anteriores con *«salidas sin gastar»*. Sin gastar implica que no se ha utilizado como entrada de ninguna otra transacción. El destino de la transacción son una o más direcciones de destino.

a) Prueba de «propiedad» del dinero

La acreditación de que se es dueño de ese dinero requiere presentar una *prueba*. La prueba se hace mediante firma electrónica.

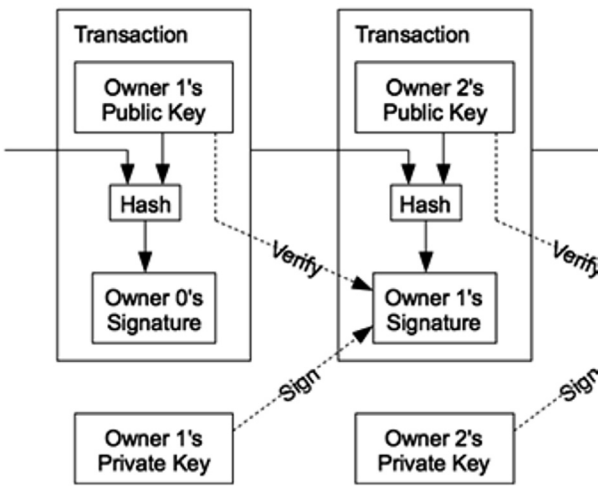
Se envía la transacción junto con la firma electrónica para cada una de las entradas, si tienen direcciones distintas. La firma incluye la clave pública de la dirección a la que pertenece.

b) Verificar una transacción

La verificación de una transacción requiere la comprobación de dos extremos.

De una parte, la constatación de que la clave pública corresponde con la dirección, repitiendo el proceso sobre la clave pública que genera una dirección unívoca. De otra parte, corroborar que la clave pública permite verificar la firma, si permite verificar que el firmante es dueño de la transacción anterior.

Ejemplo de verificación de transacción[9]



[9] Fuente: *https://bitcoin.stackexchange.com/questions/69082/how-do-transactions-in-the-block-chain-work*.

c) *Blockchain* y transacciones

El *Blockchain* es una cadena de bloques donde cada bloque está ligado al bloque anterior. Como antes hemos señalado, se pueden añadir bloques a la cadena, pero la tecnología no permite eliminar ni modificar un bloque existente.

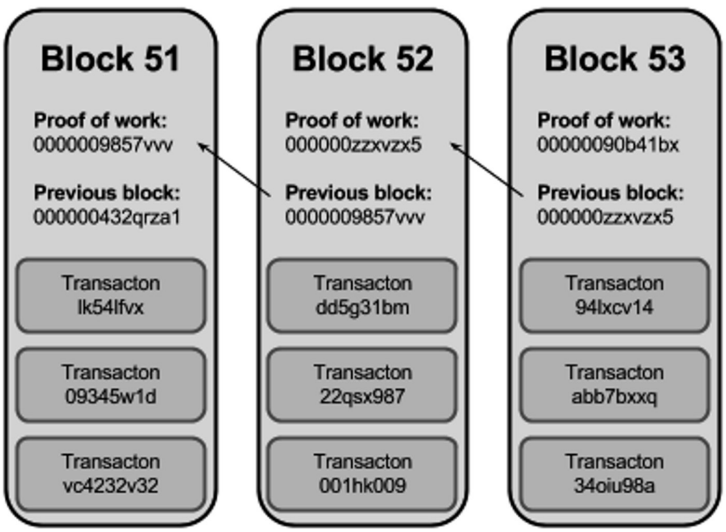
Los bloques están ligados mediante mecanismos de criptografía de forma que cualquiera pueda comprobar la veracidad de la cadena. Cada uno de los bloques contiene un conjunto de transacciones. Todas las transacciones de *Bitcoin* se almacenan en el *blockchain*.

d) Relación entre bloques y transacciones

Cada bloque contiene su «prueba de trabajo» (*proof of work*) y el del bloque anterior.

El *proof of work* se puede verificar de forma sencilla. Dado que cada bloque contiene «N» transacciones en un número cierto y conocido, no se puede modificar un bloque intermedio sin romper la cadena.

Cadena de bloques y transacciones[10]



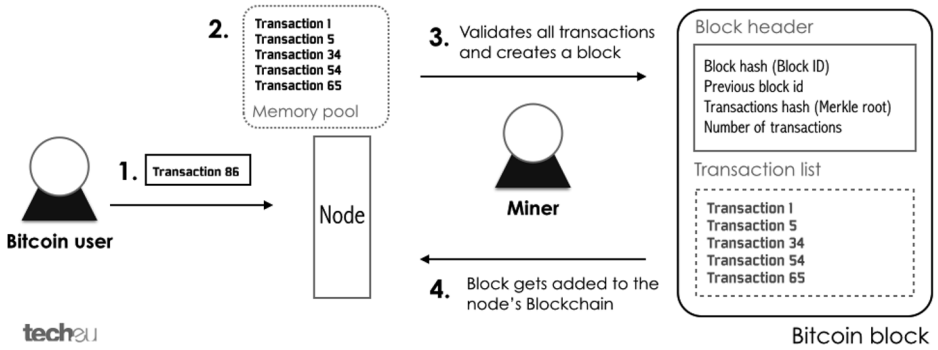
[10] Fuente: Daniel Martinez. *https://danims.com/bitcoin-vii-son-seguros-los-bitcoins/*.

e) Ciclo de vida de una transacción

Iniciado el proceso, el cliente envía la transacción a la red que la distribuye. La transacción llega a uno o varios nodos «mineros», cada minero verifica la transacción antes de aceptarla.

Cuando un minero tiene suficientes transacciones para formar un bloque, intenta resolver el puzzle de la *prueba de trabajo*. Cuando un minero lo resuelve, se envía a la red el nuevo bloque. Los «full node» verifican el bloque contra el último bloque validado. Si todo es correcto, se almacena el nuevo bloque. Una vez la transacción está en un bloque «aceptado», se considera confirmada.

Ejemplo de ciclo de vida de una transacción[11]



f) ¿«Prueba de trabajo» (*Proof of work*)?

La red de *bitcoin* es descentralizada, como el propio *Blockchain*.

Para *confirmar* una transacción todos los nodos de la red deben ponerse de acuerdo, hace falta un «consenso». La red tiene «cientos de miles de nodos», por lo que no pueden hablar todos entre sí para ponerse de acuerdo.

Para resolver este problema y alcanzar ese acuerdo, el consenso se consigue mediante «competición» de mineros utilizando el mecanismo de «prueba de trabajo» (*proof of work*). El primero que *«resuelva el bloque»* gana y todos los demás lo aceptan como válido.

En la prueba de trabajo se produce una compensación de los mineros. Los mineros «ganan dinero» cada vez que «minan un bloque» y ese bloque pasa a ser parte del *blockchain*. Es decir, si son los «primeros» en minarlo.

---

[11] Fuente: Techeu. *http://tech.eu/features/808/bitcoin-part-one/*.

Todos los «transaction fees» (salarios de transacción) de cada transacción se asignan al minero. Además cada vez que se mina un bloque se genera «nuevo dinero» (inflación) que también se asigna al minero que ha minado el bloque.

E) *Tipos de* blockchain. Blockchain *genéricas*

Existen tres tipos diferenciados de cadenas *Blockchain* con diferentes requisitos técnicos: cadenas públicas, cadenas privadas y cadenas laterales.

La cadena pública es aquella que se encuentra abierta a cualquier dispositivo y usuario. Generalmente utilizan consenso con «Proof of Work», si bien es muy criticada, ya que provoca alto gasto de energía. Además, tiene el problema de la necesidad de que debe poner de acuerdo a un gran número de actores para cualquier cambio.

La cadena privada es la cerrada a un conjunto de actores. Normalmente un conjunto de empresas, donde cada una está representada con una cantidad baja de nodos (de uno a tres). Generalmente utilizan el sistema de «prueba de participación» (*proof of stake*) para lograr consenso. Tiene la ventaja de ser energéticamente eficiente y de que los cambios pueden realizarse poniendo de acuerdo a menor número de actores.

a) Protocolos de consenso

Los mecanismos de consenso en *Bitcoin* son des-centralizados. Permiten mantener un estado global y actualizado de la red. Asimismo, deben ser «tolerantes a fallos bizantinos»[12].

Los mecanismos de consenso pueden agruparse en dos grandes grupos: de un lado, la «prueba de trabajo» (*proof of work*) y, de otro, la «prueba de participación» (*proof of stake*).

El protocolo de consenso de «prueba de trabajo» consiste en que la información de confiabilidad corrobora que el validador ha resuelto un algoritmo complejo de resolver.

Su ventaja es que evita que una sola persona envíe muchas transacciones a la red. Pero tiene los inconvenientes del elevado gasto computacional, del elevado gasto energético y de que es necesario mantener alta la dificultad del algoritmo.

---

[12] Cfr. Pérez Solà, C., & Herrera Joancomartí, J. (2014), *Bitcoins y el problema de los generales bizantinos*.

Para dominar la red es necesario tener mayor poder de computación que el total del resto de actores.

En cambio, el protocolo de consenso de «prueba de participación» surge para intentar resolver el malgasto de recursos de los algoritmos *proof of work*. En este caso, la información de confiabilidad verifica que el validador apuesta a que la transacción es correcta.

La principal ventaja es el bajo gasto energético unido a la inferior latencia de la prueba de trabajo, pero tiene el inconveniente de que la elección del concepto que se apuesta es difícil en redes públicas.

Así, la asignación de la apuesta obedece a diferentes tipos de concepto: desde la asignación estática (redes privadas), pasando por prueba de participación, hasta depósito de seguridad.

b) Permisos en el *Blockchain*

Las clases de permisos en el *Blockchain* son un aspecto importante, especialmente en aras de la seguridad y confiabilidad del sistema.

En atención a las clases de permiso, las redes públicas no tienen permisos (*permissionless*) y cualquier usuario se puede unir y participar en la red. Sin embargo, las redes privadas pueden tener permisos (*permissioned*) y los usuarios son conocidos *a priori* y se puede definir su rol con diferentes tipos de permisos (permisos para validar transacciones, permisos para desplegar contratos, permisos para invocar transacciones, permisos para registrar nuevos usuarios).

Más adelante abordaremos la privacidad en el *Blockchain*, pero cabe adelantar que el sistema permite que uno o varios participantes realicen transacciones que no sean accesibles por los demás. No obstante, igualmente hay que advertir que en casi todas las redes públicas la privacidad no existe y todos los participantes pueden ver toda la información de todas las transacciones.

Aún así, cabe mantener el «anonimato»[13] ya que no hay forma de relacionar la cuenta con el usuario.

---

[13] En este sentido conviene tener en cuenta el Considerando 26 del el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 (Reglamento general de protección de datos, RGPD). Determina que *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*

Algunas redes ofrecen soporte a la privacidad y soportan la realización de transacciones privadas. En estos casos, los datos no son accesibles y cada transacción genera una clave de encriptación diferente: de una parte, las claves públicas son conocidas por el emisor; de otra, la clave de encriptación se encripta con la clave pública de cada uno de los participantes y, finalmente, únicamente los participantes pueden desencriptar los datos de la transacción.

5. Smart Contract

A) *Concepto*

Smart Contract o Contrato inteligente es un término que aparece relacionado con el *Bitcoin*, las criptomonedas y el *Blockchain*. Pero para saber qué son exactamente los contratos inteligentes conviene entender la evolución de los contratos tradicionales.

Al pensar en un *contrato* prácticamente se piensa en un característico documento en papel con una serie de condiciones escritas, cláusulas que las partes intervinientes aceptan y expresan su firma como aprobación y compromiso de cumplir dichas estipulaciones.

Sin embargo, la incidencia de la tecnología ha propiciado la aparición hoy en día de nuevos modos contractuales, como contratos de firma digital o que requieren confirmación por voz.

Los contratos de firma digital son aquellos que se formalizan mediante el registro en un sitio web en el que finalmente se exige una cláusula del tipo *«Acepto las condiciones de uso y política de privacidad»*. La aceptación de dichos términos comporta la firma automática de ese contrato a través de ese sitio web. Su utilización alcanza cualquier portal de bienes y servicios, como por ejemplo en redes sociales como Facebook o LinkedIn, tiendas *online* como Amazon o plataformas de servicios como Airbnb.

---

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.

Sin embargo, el Considerando 28 del RGPD destaca que *La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.*

El artículo 4.5 del RGPD define la «seudonimización» como *«el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable»*.

Por otra parte, los contratos que requieren una confirmación por voz son aquellos en los que la firma es la propia voz de la persona que acepta los términos del contrato. Suele ocurrir con proveedores de servicios generales, por ejemplo, con compañías de telecomunicaciones o de suministro eléctrico. Estas compañías llaman para ofrecer un servicio con unas condiciones. Si el usuario está conforme con esas condiciones, la compañía registra los datos legales de esa persona (nombre, dirección, DNI, …) y le hace responder «acepto las condiciones», grabando su respuesta como «firma» del usuario. Pese a los nuevos formatos tecnológicos, estos contratos mantienen la esencia tradicional de contrato.

B) *Evolución de la contratación tradicional a la inteligente*

Sin embargo, actualmente la contratación evoluciona hacia los llamados contratos inteligentes, que requieren explicar detalladamente qué son, cómo se ejecutan y cuáles son sus aplicaciones, precisamente para entender mejor su relación con el *Blockchain*.

Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes de modo que ciertas acciones se efectúan como resultado de que se cumplan una serie de condiciones específicas.

Esto es, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente. Aquí estriba la diferencia con los contratos tradicionales, no sujetos a tal «automatismo», pues los *Smart Contracts* son contratos que se ejecutan y se hacen cumplir a sí mismos de manera automática y autónoma.

Los contratos inteligentes se comenzaron a desarrollar en el año 1993, cuando el famoso criptógrafo Nick Szabo[14] acuñó el término por primera vez. Nick propuso este sistema de contratos ya entonces a pesar de que la insuficiente infraestructura tecnológica del momento lo hacía inviable. Fue necesario esperar a que un sistema de pagos permitiese llevar a la práctica y esa situación apareció en escena con la creación del *Bitcoin* en el año 2009. No obstante, *Bitcoin* sólo estaba pensado para ser una herramienta financiera: una criptomoneda.

En cambio, la tecnología con la que funcionaba *Bitcoin*, el *Blockchain* o *cadena de bloques* sí que hacía posible estos contratos inteligentes. A principios de 2014, con la creación de Ethereum[15], por fin los contratos inteligentes

[14] Käll, J. (1991). «Blockchain Control». *Law and Critique*, 1-8.
[15] Cfr. *https://www.ethereum.org/foundation*.

pasaron a ser una realidad. Estos *smart contracts* «viven» en una atmósfera no controlada por ninguna de las partes implicadas en el contrato, en un sistema descentralizado. Estas propiedades son interesantes a la hora de pensar una aplicación del *Blockchain* en el ámbito de las fundaciones, particularmente en el Registro y el Protectorado, donde la relación contractual pasaría a ser una relación de la Administración Pública con la fundación.

Por tanto, en los contratos inteligentes se programan las condiciones, se firman por ambas partes implicadas y se «coloca» en una *Blockchain* para que no pueda modificarse. De forma análoga, en el ámbito fundacional público, tanto del Registro como del Protectorado de fundaciones, se podrían preestablecer las condiciones de cada trámite, se firman por las personas autorizadas, tanto de la Administración Pública como de las fundaciones, y se introduce en una *Blockchain* para que quede registrado de forma permanente a efectos oficiales.

Al igual que ocurre en todo contrato inteligente, el objetivo principal, también aplicable al ámbito de las fundaciones, es implementar un estado de seguridad jurídica superior al del contrato tradicional, reducir costes y reducir el tiempo asociado a esta clase de interacciones, lo cual redundaría en una mayor eficiencia de la Administración Pública relacionada con las fundaciones. En el caso de los *Smart Contracts,* se busca mejorar los contratos actuales siendo más seguros, más baratos, con ahorro de tiempo y con protección frente al fraude.

Cabe plantearse la disyuntiva entre contratos tradicionales y contratos inteligentes. Para mayor objetividad basta analizar la situación actual y mirar hacia el futuro. Cuando se habla de los contratos en papel, se sabe que se encuentran escritos en un lenguaje propio de las personas: se puede escribir en cualquier idioma, pero en un lenguaje legal comprensible entre dos personas. Una vez que se aceptan los términos y se firma el contrato, según las leyes aplicables, la responsabilidad y validez legal para ambas partes tiene unos costes elevados y normalmente requieren la intervención de fedatario público, como un notario, a fin de revestir de validez a ese contrato. Asimismo, y es importante, el modo de cumplimiento depende del punto de vista de cada parte implicada: en un contrato, las cláusulas tienden a beneficiar a una de las partes por encima de la otra.

Por el contrario, los contratos inteligentes difieren en los tres aspectos mencionados. El lenguaje no es natural, sino que es un lenguaje virtual, un lenguaje de programación informática. De igual manera que un programa de ordenador o una aplicación móvil se programa a fin de que ejecute una serie de funciones, los *Smart Contracts* configuran la realización de unas tareas

conforme a unas instrucciones y condiciones introducidas previamente. En consecuencia, el cumplimiento de los contratos inteligentes no permite diversos puntos de vista, sino una aplicación y ejecución objetiva. Si se da la condición establecida (normalmente bajo la estructura informática «si…, entonces…»), el contrato ejecuta automáticamente la consecuencia de dicha acción. Finalmente, la responsabilidad legal del *smart contract* sigue en análisis, pero es indudable que no requiere de un intermediario (como el notario o cualquier otro fedatario público), pues el contrato en sus términos es el intermediario de confianza, con reducción de costes y del tiempo de las interacciones. Y si se piensa en el Registro y Protectorado de fundaciones cabría vislumbrar un procedimiento administrativo inteligente con similares propiedades que los *Smart Contracts.*

C) *Funcionamiento de los Smart Contracts*

Para facilitar mejor la comprensión del *Blockchain* y de los *Smart Contracts* en el ámbito de la Administración pública, conviene conocer cómo funcionan los *Smart Contracts*. Nos serviremos de un ejemplo. Nos situamos ante una máquina expendedora de comida como las que podemos encontrar en cualquier aeropuerto o en una estación de tren. Esa máquina está programada para que cuando se introduzca una cantidad de dinero y se pulse una combinación de números, automáticamente el producto seleccionado salga de la máquina para ser del comprador. Además, otra orden que tiene programada es la de que, en caso de introducir más dinero del que costaba el producto, la máquina devuelva el cambio, y en el caso de no haber un producto seleccionado marque en la pantalla «Producto Agotado». Esta programación de la máquina es lo que sería el contrato inteligente, y las partes implicadas son la máquina y el comprador.

Las reglas del contrato inteligente son las reglas que hemos mencionado anteriormente y que son ejecutadas por sí solas si se cumplen las acciones correspondientes. Esto funciona en el lenguaje informático como una sentencia llamada *«if – then»*, que significa *«si… entonces…»* y viene a simbolizar que: *«si se cumple el acuerdo… entonces se da la condición»*. En el ejemplo anterior, estos acuerdos con la sentencia «if – then» se cumplirían del siguiente modo: si se cumple que el usuario introduce dinero suficiente y pulsa la combinación «123», entonces saldrá la botella de agua. Si se cumple que el usuario ha introducido más dinero que el necesario, entonces se le devuelve la diferencia. Si el usuario introduce el dinero y pulsa «123» pero no hay artículo, entonces aparecerá el mensaje de «Producto Agotado». Así funcio-

naría un contrato inteligente y es muy interesante pensar este modo de funcionar en la Administración pública.

Se puede pensar que estas máquinas existen desde hace muchísimos años. Pero ¿qué novedad aparece ahora? La novedad sería adelantarse un paso más y mediante el contrato inteligente programar este tipo de máquinas con la condición informática de que *«si se acaba el producto "032"… entonces —de forma autónoma y automática— la máquina mandará una señal al proveedor de botellas de agua para que vaya a reponerlas»*.

En consecuencia, se suprime a un intermediario que tenga que estar vigilando la máquina, llamando a los proveedores y reponiéndola por sí mismo, eliminando así también los costes de tiempo y dinero en dicho proceso y simplificando mucho más la tarea.

Otro ejemplo de carácter traslativo de bienes podría ser el alquiler de una propiedad. Gracias a la tecnología, en la actualidad se cuenta con cerraduras electrónicas de apertura con tarjeta, como las que se utilizan en numerosos hoteles y empresas a lo largo del mundo. Así, mientras la tarjeta asociada a la puerta esté activa, se puede entrar y salir. En el caso del hotel, imaginemos cómo sería con un contrato inteligente: si se ha pagado hasta el día 30 del mes en curso y las normas del hotel son que se tiene que salir antes de las 12:00 de la mañana, la tarjeta funcionará hasta el día 30 a las 12:00 de la mañana. A las 12:01h ya no se podrá abrir la habitación con esa tarjeta. Esas serían las reglas del contrato inteligente que se ejecuta por sí mismo una vez pasada la hora fijada. Esto haría posible un Airbnb pero sin su mediación ni sus comisiones. Y lo mismo podría pasar con plataformas como Uber o Blablacar: actuar directamente entre la gente interesada (relaciones P2P, *peer-to-peer*, entre pares), mediante un contrato inteligente, con ahorro de las comisiones de dichas plataformas y del tiempo de gestión.

Se trata de ejemplos limitados pero muestran las ventajas y posibilidades de aplicación del *Blockchain* y de los *Smart Contracts*, que abren todo un extenso panorama de aplicación legal, contractual y administrativa para el que aún no es fácil contar ya con las herramientas necesarias. No obstante, la idea fundamental es clara: un contrato inteligente funciona de forma que las partes configuran los términos del contrato, éste se almacena en *Blockchain* y, cuando se dan los términos descritos, el sistema ejecuta el contrato y se dan las consecuencias descritas en él.

Los *Smart Contracts* ofrecen un almacenamiento para datos y código, que será ejecutado y comprobado en cada transacción. Cada transacción invocará a una rutina del código que modificará estos datos. El código es inmutable

de forma unilateral. En lugar de verificar una transacción monetaria en cada transacción, se verifica el estado de la memoria tras ejecutar la rutina vinculada a la relación contractual.

Conviene clarificar que un *Smart Contract*, por lo general, no representa un único acuerdo legal. En los *Smart Contract* se representa el flujo que se ha de seguir para formalizar y realizar todos los acuerdos legales y además los elementos (propiedad, balance…) que se modifican como consecuencia de ellos[16].

Es interesante verlo en un ejemplo[17]. En el caso de una compraventa de inmuebles en *blockchain*, no habría un *Smart Contract* por cada inmueble, sino que el único contrato debería incluir los siguientes aspectos:

a) Un «registro» de inmuebles por propietario (referencia catastral por cada titular catastral).

b) Un «registro» de notarios (y una forma de modificarlos, por ejemplo, permitir que solo el colegio de notarios los modifique).

c) Las siguientes rutinas con los permisos y validaciones adecuados (vendedor es el propietario, notario es el fedatario, el registrador practica la inscripción registral, el Catastro efectúa la posterior alteración de titularidades, etc.):

- Dar de alta nueva compraventa (sistema).
- Firmar compraventa (comprador).
- Firmar compraventa (vendedor).
- Firmar compraventa (notario).
- Cuando termina el flujo de firmas, el *Smart Contract* modificaría su registro de inmuebles y cambiaría el propietario, sin perjuicio de las competencias legalmente atribuidas al Catastro Inmobiliario y al Registro de la Propiedad[18].

---

[16] Salvador Sáez, D. (2018). «Las monedas virtuales y el capital riesgo: realidad, función económica, naturaleza y consideraciones jurídicas sobre el *Bitcoin*». *Revista Española de Capital Riesgo*.

[17] Código de Smart Contract compraventa a distancia segura con «Solidity» en Ethereum: *https://solidity-es.readthedocs.io/es/latest/solidity-by-example.html#compra-a-distancia-segura*.

[18] Cfr. Ley 13/2015, de 24 de junio, de Reforma de la Ley Hipotecaria aprobada por Decreto de 8 de febrero de 1946 y del texto refundido de la Ley de Catastro Inmobiliario, aprobado por Real Decreto Legislativo 1/2004, de 5 de marzo (2015). Boletín Oficial del Estado. Recuperado a partir de *http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-7046*.

D) *Figura del «oráculo» (*oracle*)*

Los *Smart Contracts* han puesto de moda un concepto no siempre claro como el de «oráculo» (*oracle*). Para entenderlo mejor y comprender la importancia que puede llegar a tener en el ámbito de la Administración pública, y concretamente de las fundaciones, puede ayudar el siguiente ejemplo.

Borja y Juan son aficionados al fútbol. Borja es del Real Madrid y Juan es del FC Barcelona. Borja quiere apostar 5 Ether (la criptomoneda de *Ethereum*) a que el Real Madrid gana el disputado clásico y Juan quiere apostar los mismos Ether a que lo gana el FC Barcelona. Como son personas de hechos más que de palabras, llevan a cabo desde su móvil la apuesta a través de un contrato inteligente, especificando las reglas del contrato y depositando los fondos en una cuenta. Una vez que se sepa quién gana, el contrato repartirá a uno u otro el total de Ether apostados automáticamente. En este caso un ente externo al contrato tiene que confirmar a éste quién ha ganado y ese ente es el «oráculo» (*oracle* en inglés). Esta herramienta tecnológica permite actualizar el estado de los contratos inteligentes con información externa, como por ejemplo qué equipo ganó el partido.

Ciertamente ese órgano es un externo a la cadena de bloques o *blockchain*, es un tercero, un intermediario en el que se debe confiar. Por lo tanto, tiene un impacto en el aspecto de centralización, algo totalmente opuesto a la tecnología *Blockchain*. Para solucionar esta introducción de un intermediario en la cadena y descentralizar la obtención de este resultado, hay proyectos que actúan como portadores de información entre los servicios externos (API's) y *Ethereum*. Un ejemplo es Oraclize[19]. Este proyecto combina todos los portales de información que sean indicados en el contrato y establecidos como relevantes, y es Oraclize quien, en función de los resultados que obtenga, tomará su decisión final. En efecto, no valoramos ahora la fiabilidad o seguridad jurídica de entidades y oráculos que son terceros de confianza.

E) *Funciones adicionales de los* Smart Contracts

A la hora de ampliar la utilización de los contratos inteligentes, y no sólo en el ámbito de las relaciones particulares, sino si los pensamos en el seno de la Administración Pública en general y de la relacionada con las fundaciones en particular, resulta fundamental tener en cuenta la función multifirma de los *Smart Contracts*. Es una función mediante la que dos o más personas se deben poner de acuerdo para hacer cumplir las condiciones de un contrato.

[19] Cfr. *http://dapps.oraclize.it/*.

En consecuencia, a través de la función multifirma las diversas personas intervinientes en el contrato tienen que estar de acuerdo, de modo que ninguno pueda beneficiarse unilateralmente ni perjudicar conjuntamente al resto de intervinientes.

Otra función interesante de los *Smart Contracts* es la de los dobles depósitos y actuaciones similares. Esta característica de los contratos inteligentes hace que funcionen correctamente, eliminando al intermediario del proceso. Permite a dos o más partes que no se conocen entre sí y que carecen de confianza recíproca, realizar una transacción segura para ambos a través de un contrato inteligente. Este contrato les obliga a depositar en una dirección de la cadena de bloques unos fondos para el cumplimiento del contrato. El contrato tiene una duración determinada, y si no llegan a un acuerdo, el contrato inteligente remitirá directamente los fondos que ambas partes tuvieron que abonar a otra dirección de la cadena de bloques de la que nadie podrá sacarlos nunca. Esta condición fuerza a cumplir a cada uno con su parte del contrato. De lo contrario, los fondos desaparecerían. En conclusión, este doble depósito hace que sea imposible que una de las partes gane sin que la otra lo haga, es decir, no se dan engaños y hace que la gente llegue a acuerdos amistosos. Este tipo de métodos ya se han añadido en algunos mercados descentralizados. Los podemos ver en portales como Bithalo y Black Halo.

F) *Usos de los contratos inteligentes*

La actual plataforma Ethereum, la tecnología *blockchain* y los contratos inteligentes son herramientas novedosas, pero entendemos que los usos de los *Smart Contracts* actualmente no representan, ni mucho menos, los usos que tendrán en un futuro próximo.

Al igual que Internet nunca se pensó para mandar correos electrónicos y, sin embargo, hoy día continúan apareciendo permanentemente nuevos usos de la «Red de Redes», los contratos inteligentes se podrán aplicar a prácticamente todas las cosas. De alguna manera, serán el vehículo de la transformación del Internet actual, para pasar de una Red de Información a una *«Red de Valor»*.

Para ayudar a tomar conciencia de los usos que los *Smart Contracts* pueden ofrecer y, de este modo, vislumbrar la potencialidad que la tecnología *Blockchain* puede tener también en la Administración pública, enumeramos algunos ejemplos por sectores.

Entre los servicios financieros, podemos encontrar los siguientes usos. 1) Préstamos: si la persona que contrata el préstamo no realiza el pago en el tiempo estipulado, se ejecutaría el contrato para retirarle las garantías. 2) Liquidación de operaciones: los contratos calculan importes de liquidación y transfiere fondos automáticamente. 3) Pagos de cupones y bonos: los contratos calculan y pagan automáticamente de forma periódica los cupones y devuelve el capital al vencimiento de los bonos. 4) Microseguros: Calculan y transfieren micropagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotriz de pago por uso). 5) Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y, una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor. 6) Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, las propiedades quedan repartidas y asignadas automáticamente entre los herederos. 7) Automatización de pagos y donaciones: se pueden acordar pagos o donaciones periódicas o puntuales a personas o entidades. El contrato inteligente verificaría que se cumplen las reglas para realizar automáticamente la donación.

En el sector de los Servicios de la salud, algunos casos de uso son elocuentes: 1) Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores. 2) Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micropagos automáticamente al paciente para su participación. 3) Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos IoT (*Internet of Things*) conectados a Internet. Los contratos generan automáticamente las acciones necesarias basadas en hechos específicos, como la concesión de citas o la remisión de medicamentos de receta necesaria directamente desde el depósito farmacéutico.

También los Servicios de propiedad intelectual permitirían usos significativos de contratos inteligentes, como la distribución de *royalties*. El *smart contract* calcula y distribuye los pagos de *royalties* a artistas y otras partes asociadas según los términos acordados.

En el sector de los servicios energéticos ya son una realidad las estaciones autónomas de recarga para vehículos eléctricos: el contrato procesa un depósito, habilita la estación de recarga y devuelve los fondos restantes una vez completados.

Y entre los servicios del sector público, podemos destacar los siguientes. 1) Votación: valida los criterios del votante, registra el voto en la cadena de bloques e inicia acciones específicas como resultado del voto mayoritario. Esto es posible en una votación tanto de encuesta como estatal. 2) Apuestas: dos o más partes pueden apostar con seguridad tecnológica y jurídica, y sin necesidad de un tercero, a través de un contrato inteligente que asegure unas condiciones concretas. 3) Propiedades inteligentes: una casa, un coche, una nevera, una lavadora…todos los objetos que se puedan conectar a Internet se consideran propiedades inteligentes (del inglés, *smart property*). Y todos pueden ser gestionados con contratos inteligentes para poder venderlos, alquilarlos y gestionarlos de forma automatizada. Así, el vehículo que tenga su ITV en el plazo de renovación podría solicitar automáticamente cita previa y recibir la confirmación de haber pasado satisfactoriamente el proceso de revisión.

G) *Beneficios de los contratos inteligentes*

A la vista de la definición y de la amplitud de posibilidades jurídicas que ofrecen los *Smart Contracts*, el análisis sucinto de sus beneficios puede ayudar a valorar el interés de su aplicación, pues el Derecho ya ha estudiado ampliamente en sede de obligaciones y contratos tradicionales las consecuencias de su incumplimiento, que se aplicarían de igual manera a los inteligentes.

A) Autonomía. Estos contratos se dan siempre entre una o varias personas físicas o jurídicas, pero en principio sin ningún intermediario. No es necesario que alguien valide el contrato, aunque en función de su complejidad podría ser necesaria la orientación y experiencia de un abogado. Por ello, con carácter general reducen e incluso pueden llegar a eliminar cualquier persona extra que no esté implicada en el contrato.

B) Costes. Los contratos inteligentes al no depender de la intervención de terceros, reducen notablemente los costes. A menor intervención humana, mayor reducción en costes.

C) Confianza. Todos los contratos inteligentes van directos a la cadena de bloques. Esto hace que 1) esté encriptado, por lo que únicamente las personas implicadas pueden acceder a su contenido y leerlo; y 2) permite la interacción entre personas que no se conocen entre sí y sin que haya riesgo de estafa.

D) Velocidad. Los contratos inteligentes utilizan código de software para automatizar las tareas que, de otro modo y como en los contratos tradicionales, se realizarían por medios manuales. Por lo tanto, aumentan la velocidad

de los procesos de negocio y son menos propensos a errores humanos o manuales.

E) Seguridad. Los contratos inteligentes basados y securizados en la cadena de bloques pública no pueden perderse. Todo queda registrado de forma inmutable. Nada ni nadie los puede hacer desaparecer por su sola voluntad y siempre se tiene acceso a ellos, sin perjuicio de las implicaciones en privacidad. El proceso de ejecución descentralizado elimina el riesgo de manipulación, ya que la ejecución es gestionada automáticamente por toda la red, en lugar de por una parte individual.

F) Nuevos modelos de negocio. Los contratos inteligentes, a través de sus bajos costes para asegurar transacciones confiables, permiten nuevos negocios, como el acceso automatizado a vehículos y unidades de almacenamiento. Esto puede abrir nuevas vías de emprendimiento si se suma a otras tendencias emergentes como el Internet de las cosas (IoT) o tecnologías disruptivas como los vehículos autónomos o la robótica.

H) *Implicaciones*

A modo de conclusión, con muchos otros expertos y especialistas en esta materia, suscribimos que los contratos inteligentes entrarán a formar parte de nuestra vida cotidiana y en multitud de sectores y esferas, como ya lo ha hecho el Internet de la Información.

La implicación más evidente y ya en la actualidad puede ser la sustitución de los contratos tradicionales elaborados a través de abogados por la transformación en plantillas estandarizadas de contratos inteligentes. Una variante puede ser la integración de contratos inteligentes en un híbrido de papel y contenido digital, donde los contratos se verifican a través de *blockchain* y se corroboran mediante copia física.

Sin embargo, una de las implicaciones de amplio alcance de los contratos inteligentes puede encontrarse en la Administración Pública, con una creciente sustitución y mejora de los procedimientos tradicionales por procedimientos inteligentes, con la innovación y eficiencia que ello podría comportar en general.

Finalmente, no hay duda de que en aquellas áreas donde se precise una comunicación entre dos o más partes, ya sean estas personas físicas vivas o máquinas, este tipo de contratos permiten que esa comunicación sea cien por cien veraz, segura, rápida y de bajo coste, con las ventajas que ello generaría para los sectores privado y público.

6. *El* Blockchain *en el entorno digital*

El *Blockchain* comenzó con el *Bitcoin*, pero en la actualidad no es sólo ni únicamente un medio de pago[20]. Sus desarrollos tecnológicos adquieren mayor relevancia como infraestructura y plataforma que como criptomoneda[21]. *Blockchain* es sinónimo de criptología y algoritmos[22].

En este nuevo marco surge una innovadora cultura empresarial basada en *Blockchain*. Hoy muchos sectores sociales y económicos buscan casos de uso y negocio basado en *Blockchain*. La innovación principalmente se está produciendo en dos campos: el primero, en la forma de interacción, con especial relación con quien envía los datos; y el segundo, en la transmisión de datos, en particular la arquitectura de distribución: cómo se envían los datos, con la interacción hombre-máquina, objeto de evolución de las últimas décadas.

Entre las singularidades del impacto del *Blockchain* en el ámbito económico y social podríamos destacar el siguiente marco de cuatro pilares:

a) Datos, información y conocimiento.

b) Industrialización, que hará que Internet no sea intercambio de información sino de bienes.

c) Infraestructura para el modo de uso de la información con mayor impacto social, con una herramienta nueva ahora todavía en la fase de diseño.

d) Nueva herramienta de impacto escalable.

Con este nuevo sistema, se ha cambiado la forma de intercambio de la información. *Blockchain* es un *«registro digital distribuido (LEDGER), que garantiza la autenticidad, de manera única con la integridad y el reconocimiento de la propiedad de los activos y las transacciones digitales»*.

Es una transmisión de información por bloques a todos los nodos caracterizada por las siguientes dos propiedades. Es *«centralizada»*, de modo que físicamente todos los actores están geográficamente distribuidos y jerárquicamente todos los actores tienes poder de acción y decisión sobre la red. Es *«inmutable»,* pues *a priori* y técnicamente no se puede modificar. Es segura,

---

[20] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. «O'Reilly Media, Inc.».

[21] Zyskind, G., & Nathan, O. (2015, May). «Decentralizing privacy: Using blockchain to protect personal data». In *Security and Privacy Workshops* (SPW), 2015 IEEE (pp. 180-184). IEEE.

[22] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). «Hawk: The blockchain model of cryptography and privacy-preserving smart contracts». In 2016 *IEEE symposium on security and privacy* (SP) (pp. 839-858). IEEE.

tanto en su infraestructura como en su software (ejemplo: aplicaciones de compartición de archivos seguros).

Adelantamos que dichas propiedades pueden ser tenidas en cuenta a la hora de pensar en los registros públicos y, más específicamente, en el ámbito del protectorado y registro de fundaciones, pues con sus peculiaridades territoriales tienden a estar centralizados y son inmutables.

No obstante, el potencial disruptivo de *Blockchain* estriba, como también podría ocurrir en el ámbito de la Administración Pública electrónica, en cuatro notas fundamentales: (1) supervisión, (2) confiabilidad, (3) resiliencia e (4) innovación. Desde una perspectiva cualitativa, el *Blockchain* supone de forma segura el cambio del valor y del rol intermediario, y desde un enfoque cuantitativo se pronostica un crecimiento de 2.300 millones de dólares estadounidenses para el año 2021[23].

Por esta razón en este nuevo entorno conviene familiarizarse con dos nuevos conceptos que, pese a su importación terminológica del inglés como neologismos, ya son habituales en el *Blockchain*: *token* (símbolo) y *tokenización*.

Significa representar activos empresariales, desde objetos físicos hasta instrumentos financieros y propiedades, en *Blockchain* mediante *símbolos digitales* para agilizar sus transacciones y transferencias. Las propiedades y funciones de cada *token* estarán completamente sujetas al uso de que se establezca para ellos.

Un buen ejemplo lo constituye el *«intercambio de diamantes de sangre, Sudáfrica-Londres»*, a través de *Smart Contracts* (cláusulas contractuales); firmas de políticas, verificación de pago, etc. Todo lo que sea numéricamente una verdad, se puede ejecutar en el *Blockchain*.

7. *Valor del* Blockchain*: «Internet del valor»*

En la actualidad ya se reconoce el valor económico, social y jurídico del *Blockchain*. Su interés alcanza desde el entorno comercial y con ánimo de lucro hasta las fundaciones y asociaciones sin fines lucrativos.

Blockchain es así el *Internet del valor*. Permite el intercambio seguro del *valor* (dinero, propiedades, etc.). *Blockchain* facilita conocer el origen de los bienes (valores) y también de forma segura, a través de los *Smart Contracts* permite el seguimiento de la trazabilidad y la transparencia de las transaccio-

[23] Cfr. *Size of the blockchain technology market worldwide from 2016 to 2021 (in million U.S. dollars). https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/.*

nes con independencia de su mayor o menor cuantía, lo cual es de enorme importancia jurídica tanto para las partes implicadas como para la seguridad de los actos y negocios realizados.

De ahí la importancia del *Blockchain* para el Tercer Sector, pues por ejemplo se podría efectuar una donación de dinero desde España y vincularla al seguimiento de las concretas vacunaciones que se realicen en Kenia. Todo ello además de los interesantes casos de seguimiento de proyectos de ONGD's y de los fondos a ellos destinados.

El *Blockchain* hace posible la comprobación en el destino del valor, puesto que es una gran base de datos de la información, que no estará en la propia organización, y a la cual se le dotará de inteligencia, para conocer las características y metadatos que sean necesarios en cada acto, negocio o proyecto.

Sin embargo, hacer posible la utilización de *Blockchain* comporta un problema: resolver los problemas legales de las transacciones de valor, lo cual exige un mayor cumplimiento normativo de la regulación nacional, europea e internacional, además de cambiar el modelo de *organización vertical* («de empresas») a *horizontal* («asociación, colaboración»).

El *Ecosistema 4.0* en que se desarrolla el *Blockchain* precisa tomar en consideración los siguientes aspectos:

a) El *Mundo real*, comprensivo de la producción, de nuevos servicios. El ámbito donde se produce la innovación.

b) El Mundo operacional y el Mundo de la creación, que requiere de garantías (ejemplo: en el diseño de un avión, no se pueden hacer pruebas con riesgo para los pasajeros).

c) Nuevas obligaciones de cumplimiento normativo (penal, protección de datos, financiero…): se hace necesaria la permanente supervisión.

d) *Ecosistema 4.0* = Gobierno/Sector Público + Sector Empresarial + Universidad. Cada vez es más claro que el regulador tiene que trabajar con las empresas y viceversa, al igual que se precisa una participación más colaborativa con los reguladores.

Dos épocas básicas han marcado los *networks tecnológicos*: una primera, el intercambio de información, a través de la transferencia de datos y, una segunda, el intercambio de valor, mediante la transferencia de valor.

Por ello podemos sostener que el *Blockchain* va a cambiar la tecnología y la sociedad, dando paso a un *Internet del Valor*, en el veremos surgir una Red

pública y permisionada, compatible con la regulación, sin criptomoneda embebida (con coste transaccional bajo y predecible), con un mayor rendimiento y escalabilidad, con la finalidad de la transacción (*Transction finality*) incluida en un bloque determinado y, sobre todo, una Red gobernada y regulada.

8. *Enfoque corporativo del* blockchain

A) *Las entidades en* Blockchain

Las entidades pueden emplear el *Blockchain* como una herramienta para optimizar su actividad o sus procesos corporativos. No obstante, para tener una visión de conjunto más clara, conviene valorar las características del *Blockchain* en el actual escenario digital para optimizar su implementación. En primer lugar, el *Blockchain* puede ser parte de la estrategia corporativa, como valor añadido. A ello se suma la intensa transformación digital que la tecnología ha llevado a todos los sectores y niveles sociales, empresariales, corporativos y gubernamentales.

En segundo término, si bien se trata de una tecnología emergente, cuando no disruptiva, la posibilidad de crear una colaboración global convierte al *Blockchain* en una plataforma útil en la gestión de actividades y proyectos hasta ahora implanteables o sólo asumibles con un elevado coste.

En tercer lugar, la *cadena de bloques* ya permite crear nuevas oportunidades colaborativas, de negocio y administrativas en donde la apuesta por la innovación contribuye a resolver problemas o a cubrir necesidades de forma más eficiente, rápida, segura y fiable.

B) *La «Cuarta Revolución Industrial»*

La aparición de internet en los años 80 del siglo XX supuso la irrupción de la tecnología y muchas personas quedaron fuera «del juego tecnológico» por brecha generacional, digital o de adaptación. El sector legal y administrativo no ha sido una excepción y realmente ha sido uno de los que se ha sumado tarde a las nuevas tendencias tecnológicas.

Hoy en día con *Blockchain* puede ocurrir algo similar, pues podría generar una resistencia fuerte al cambio de paradigma que puede suponer concretamente para los operadores jurídicos y para la Administración Pública.

Si *Blockchain* ya puede cambiar y está cambiando el modelo de los negocios, donde hay más interés en la transmisión de valor y activos que en la comunicación de información hasta ahora conocida, también puede irrumpir

en positivo en el área legal con contribuciones significativas para los particulares, principalmente a través de los *Smart Contracts*, y para la Administración Pública, mediante la automatización de procedimientos y procesos. Lejos de provocar una sustitución del valor humano y de las decisiones personales, precisamente descargar de burocracia innecesaria es un modo de modernizar la Administración, sustituida por procesos que pueden ejecutar correctamente las máquinas, y de crear y potenciar la importancia de las decisiones que solamente pueden adoptar los órganos administrativos unipersonales o colegiados.

A diferencia de cómo se han gestionado otros estadios tecnológicos por los operadores jurídicos, ahora es tiempo de aprender y de equivocarse, de asumir un cambio de paradigma que puede ser revolucionario para las personas y las organizaciones, de atreverse a un cambio de la mentalidad interna para adaptarse a la nueva realidad descentralizada que comporta el *Blockchain*. No obstante, como ha demostrado la Historia, este cambio no es sólo tecnológico y ha de llevar aparejado el correspondiente cambio jurídico y en el estatuto de los derechos que corresponden a las personas.

Como propuesta concreta que podemos hacer desde nuestra experiencia profesional, la aproximación jurídica al *Blockchain* puede hacerse desde una organización no jerárquica, pero sí colaborativa. Esto es, liderando desde la innovación, con conocimiento de la tecnología para hacerla segura también jurídicamente. Una digitalización que se ve acompañada del Derecho no como mera limitación sino precisamente como refuerzo de su necesidad, estrategia e implementación. En otras palabras, *aprender haciendo* («learn by doing») y de forma descentralizada y colaborativa, pero con consistencia jurídica a fin de que el diseño de la *Blockchain* del futuro sea conforme a Derecho y evite así consecuencias perjudiciales para las personas, la sociedad, las empresas y las corporaciones privadas y públicas.

Desde esta perspectiva de la seguridad jurídica, consideramos que el *sistema planetario del Blockchain* ofrece como plataforma, en el sentido de infraestructura, y como instrumento unas muy amplias posibilidades, y no sólo en el entorno monetario y financiero que es donde ha surgido el *Bitcoin* y otras criptomonedas. Por ello, puede ser de mayor interés identificar el *Blockchain* para tareas y necesidades nuevas y no solamente para lo que no funciona. Y una de las áreas extensas de interés es, sin duda, la Administración Pública en servicio a los ciudadanos, pues además de que se produce la tramitación de un elevado volumen de expedientes («transacciones»), también reúne importantes notas de *trazabilidad*, como ocurre en expedientes judiciales y en procedimientos administrativos.

A modo de ejemplo, es interesante descubrir cómo algunas entidades financieras han comenzado a gestionar la concesión de préstamos a través del potencial de esta tecnología en las finanzas corporativas[24]. Asimismo, algunas compañías eléctricas españolas también han comenzado a efectuar transacciones de energía con *Blockchain* o la filial alemana de Telefónica ha colocado deuda mediante la tecnología sobre la que se hizo *Bitcoin*. En definitiva, se asume que el *Blockchain* funciona sobre una base de datos de transacciones distribuidas entre múltiples ordenadores que resuelve dos problemas clave en el mundo digital: hacer operaciones sin necesidad de un intermediario de confianza y garantizar que esas transacciones no puedan ser alteradas, eliminadas o revertidas posteriormente.

9. *De los procedimientos administrativos a las actividades de las fundaciones*

La regulación contenida en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, no impediría la implantación del *Blockchain* en la Administración Pública, si bien en este análisis no podemos profundizar en todo su detalle. Baste como ejemplo elocuente su nuevo artículo 12, que regula la asistencia en el uso de medios electrónicos a los interesados, y dispone que *«las Administraciones Públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen»*.

Con esta habilitación legal y una Administración Pública centrada en el servicio al ciudadano, la utilización de medios digitales y de tecnologías emergentes para alcanzar un mayor estándar de cumplimiento puede contribuir a una efectiva modernización de la Administración. Aunque puedan ser necesarios ajustes normativos y procedimentales, pues el paso del papel a lo digital puede requerir algunas redefiniciones administrativas, ciertamente el soporte digital de los procedimientos administrativos puede redundar en su mayor agilizad, eficiencia y garantía jurídica, un mayor grado de cumplimiento y acierto administrativo al descargar de burocracia los procesos automatizables y al generar un mayor valor añadido en la toma de decisiones por las autoridades y órganos competentes.

---

[24] Cfr. *BBVA renueva un préstamo de 325 millones a Repsol basado en la tecnología «blockchain»*. Accesible en *https://www.publico.es/economia/bbva-renueva-prestamo-325-millones-repsol-basado-tecnologia-blockchain.html*.

De igual modo, en la relación entre la Administración Pública y los administrados, como por ejemplo las fundaciones en su interrelación con el Protectorado y el Registro de Fundaciones, las tecnologías como el *Blockchain* o los Contratos inteligentes pueden contribuir decisivamente a un mayor y más fiable intercambio de información, así como a una significativa seguridad jurídica en la que queda reforzado el papel activo del administrado como de la Administración competente en cada caso.

En este ámbito, como destaca la mayoría de los expertos jurídicos en *Blockchain*, como tecnología no se puede regular en el sentido más estricto de la palabra. Precisamente cuenta con sus propias reglas de funcionamiento. Sin embargo, sí será posible legislar todas aquellas actividades que utilizan *Blockchain* como infraestructura o como medio.

10. *Aplicación del* **Blockchain** *a las Administraciones Públicas*

A) *Perspectiva general*

La tecnología del *Blockchain* en la Administración Pública puede tener múltiples aplicaciones. Por ejemplo, el Ministerio de Justicia español ha sido pionero en su interés por *Blockchain*, pues las posibilidades que ofrece esta tecnología es mayor en función de sus características inherentes, como inmutabilidad, transparencia o flexibilidad.

De este modo, es de particular interés para la gestión y seguridad jurídica de registros públicos, privados, de la propiedad, catastro inmobiliario, padrones de viviendas, registros certificados, educativos o sanitarios.

La importancia de la aplicación del *Blockchain* en administraciones descentralizadas es crucial y, como el caso español, más en aquellas administraciones con competencias transferidas, como ocurre en la sanidad. En estas áreas el *Blockchain* puede contribuir decisivamente a simplificar y resolver incompatibilidades. Se puede pensar ya como caso real no sólo en la historia clínica electrónica sino en la gestión administrativa del Protectorado y, en cierta medida, en el Registro de Fundaciones.

De hecho, un primer ejemplo en España de aplicación de esta tecnología al sector público es el contrato del Ministerio de Justicia para el desarrollo del Registro Civil Digital, que representa hasta donde hemos podido saber el primer contrato público que menciona de manera directa *Blockchain*, ya que el pliego pide al menos un experto en esta tecnología.

Sin embargo, el análisis de la problemática, a modo de caso de estudio de la fe pública registral en el Registro de Fundaciones, la tramitación de co-

municaciones y autorizaciones del Protectorado y de la seguridad en el tráfico jurídico por parte de las fundaciones requiere soluciones mediante principios y derechos clave en el entorno digital como la privacidad, la protección de datos personales y el derecho al olvido.

B) Blockchain *y privacidad*

Ciertamente, una de las áreas de mayor impacto de la aplicación administrativa del *Blockchain* es la privacidad y podría colisionar con el Reglamento (UE) 2016/679, de 27 de abril de 2016[25] (Reglamento general de protección de datos, RGPD), aplicable desde el 25 de mayo de 2018 en todos los Estados miembros de la Unión Europea y de manera directa.

Este Reglamento pretende acabar en Europa con la fragmentación nacional de la protección de datos. Además, en España el pasado 10 de noviembre de 2017 el Gobierno aprobó el proyecto de nueva Ley Orgánica de Protección de Datos (LOPD) que ya se tramita en sede parlamentaria, sin perjuicio de la regulación anticipada en régimen sancionador por el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

Entre otros derechos como el de cancelación o portabilidad de datos, esta normativa regula el derecho de supresión (*«el derecho al olvido»*, art. 17). En su aplicación, el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento (editores digitales, proveedores de servicios de Internet, motores de búsqueda, etc.), la supresión de los datos personales que le conciernan. Y el responsable estará obligado a suprimir sin dilación los datos personales. Por consiguiente, la inmutabilidad del *Blockchain* puede entrar en conflicto con el derecho al olvido y la privacidad, al impedir la actualización o supresión de la información registrada en la cadena de bloques sin consenso de las partes implicadas.

El RGPD puede colisionar con el *Blockchain* en su hasta ahora principal utilidad o punto fuerte, que es precisamente su inmutabilidad e inalterabilidad: una vez que se introducen los datos no pueden ser borrados. El derecho al olvido reconocido en Europa contraviene directamente la idea distintiva de

---

[25] Europea, U. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos que viene a derogar y sustituir a la Directiva 95/46/CE, Diario Oficial de la Unión Europea. Diario oficial de la Unión Europea, 27.

una tecnología que hace inmutable los datos registrados. El problema se agrava ante el esfuerzo inconmensurable que supondría la modificación, eliminación o desindexación de la información registrada en las bases de datos de *Blockchain*. Esta limitación del *Blockchain*, pese a sus indudables ventajas, podría dificultar su implantación en el ámbito del sector público, concretamente en el seno del Protectorado y Registro de Fundaciones.

Algunos expertos plantean como solución que la legislación nacional de cada Estado miembro de la Unión Europea limite el alcance del derecho al olvido en los sistemas *Blockchain*, lo cual no está exento de dificultades tecnológicas y de contradicciones jurídicas, aparte el riesgo de nueva fragmentación nacional, que es lo que el RGPD pretende superar. Otros especialistas sugieren la posibilidad de desarrollar cadenas editables que permitan a uno o varios administradores reescribir o cambiar bloques de información de posición sin alterar la totalidad de la cadena, con el consiguiente peligro de falta de transparencia y de inseguridad jurídica.

Habrá que esperar a la efectiva aplicación del RGPD para valorar la viabilidad del *Blockchain* en entornos no monetarios ni financieros, así como a la iniciativa del Legislador para abordar decididamente cuestiones necesitadas de moderna regulación, como la veracidad jurídica de las transacciones, la consiguiente responsabilidad legal de los intervinientes, la validez jurídica de los documentos almacenados digitalmente y su preservación, la validez legal de los propios instrumentos financieros emitidos y las cuestiones relativas a la territorialidad y responsabilidad en los *Smart Contracts* y el desarrollo jurídico del *Internet of Things*.

No obstante, entendemos que la protección de datos y la aplicación del nuevo RGPD plantean retos que convendría examinar con el objetivo de diseñar redes de *Blockchain* que mantengan las propiedades que hacen esta tecnología atractiva, particularmente inmutabilidad y descentralización), y, a su vez, ser capaz de cumplir con la regulación europea y nacional aplicable. En este sentido, es positivo que diversas autoridades en la Comisión Europea sigan ya esta tendencia tecnológica y se acrecienta la seguridad jurídica en la utilización administrativa del *Blockchain*.

La manera de plantear una solución práctica para introducir el *Blockchain* en el ámbito público fundacional es partir de la distinción entre datos personales y no personales, especialmente en una red en la que la información compartida permanece a futuro de forma inmutable, pues los datos no personales quedan fuera del alcance de la legislación sobre protección de datos y, por tanto, del RGPD.

Llegados a este punto, para poder transformar datos personales en no personales —y evitar así la aplicación del RGPD sobre ellos—, es indispensable aplicar medidas técnicas de anonimización que impidan, de manera irreversible, la posibilidad de identificación del titular de los datos. Como hemos anticipado antes, las dos soluciones que podríamos proponer serían, de una parte, la aplicación de la función *hash* y de otra, en la línea de la descentralización, la utilización de canales privados con datos cifrados.

En resumen, la técnica del *hash* comportaría custodiar los *hashes* correspondientes a cada dato personal en la red *Blockchain*. Por su parte, los datos personales se conservarían separadamente a través de una base de datos gestionada por el responsable de tratamiento. Mediante esta tecnología, se pueden modificar o eliminar datos personales para garantizar que el interesado pueda ejercitar sus derechos de conformidad con el RGPD, y al mismo tiempo preservar los beneficios inherentes a la inmutabilidad, propiedad básica de la tecnología *Blockchain*.

De otra parte, la implementación de canales privados, como los que de alguna manera existen ya con las sedes electrónicas de la Administración Pública y el sistema de notificaciones oficiales, permitiría un mayor margen de desarrollo de la *Blockchain* pública. Los canales privados son vías de transmisión de información creadas por dos o más nodos que quieren compartir información en privado dentro la red *Blockchain*. Esto es, se podría compartir la información de punto a punto sin que los demás nodos conozcan ni tenga acceso al contenido compartido. Los nodos restantes que se encontrarían situados fuera del canal privado únicamente podría acceder y disponer del *hash* de la información que se comparta en el canal privado incluso a efectos de incrementar la seguridad técnica y jurídica, además de la transparencia.

C) Blockchain *en las actividades fundacionales*

El cumplimiento de los fines fundacionales comporta la realización de actividades por parte de las Fundaciones en las que la red *Blockchain* podría resultar de gran ayuda como prueban los diversos casos de éxito conocidos[26].

Proyectos como los del Fondo Multilateral de Inversiones[27] evidencian el interés del *Blockchain* para los llamados proyectos en «la última milla». Por ello, emplear el *Blockchain* para la disrupción en la «última milla» ayuda a

[26] Cfr. «Emplearán blockchain para integrar poblaciones vulnerables en Argentina». Accesible en *https://www.criptonoticias.com/adopcion/emplearan-blockchain-integrar-poblaciones-vulnerables-argentina/*.

[27] Cfr. *https://www.fomin.org/es-es/portada/proyectos.aspx*.

trabajar con seguridad técnica y jurídica, por ejemplo, en el último rincón de Argentina donde los agricultores no reciben el valor del producto que se quedan los intermediarios.

Por ello, en las actividades fundacionales donde sea necesario contar con la intermediación, pues muchos proyectos son de valor transferido como aportación o donación, cobra asimismo una gran importancia la identidad soberana y la trazabilidad, para asegurar que el valor transferido alcanza desde el emisor hasta el receptor, desde el donante hasta el efectivo y concreto donatario.

En definitiva, el *Blockchain* puede ser de utilidad en aquellas actividades fundacionales en las que transparencia y trazabilidad sean esenciales. Así, *Blockchain* puede alinear el impacto del proyecto, el presupuesto y los agentes implicados. Baste pensar en los modelos de pago por éxito y bonos de impacto social, ampliamente difundidos en el sector de la cooperación al desarrollo. En este ámbito, si nos atenemos al modelo de «Pago por resultados», gracias a la red *Blockchain* se podrían alinear los impactos y los resultados con los proyectos. Se resuelve además el cuello de botella entre la supervisión de lo proyectado y lo ejecutado por un tercero de confianza: lo resuelve directamente *Blockchain* de forma inmediata, en tiempo real, con transparencia y con disponibilidad de toda la información en el *Blockchain*.

11. *Conclusiones*

A modo de resumen de todo lo anteriormente expuesto, se podría concluir lo siguiente:

a) Las fundaciones pueden emplear ya la tecnología *Blockchain* como una herramienta eficaz para optimizar, tanto la propia gestión interna, como la ejecución de sus actividades específicas. Aunque esta tecnología necesita aún de un desarrollo técnico y jurídico adecuado que la haga accesible a la generalidad de este tipo de entidades.

b) *Blockchain*, como *cadena de bloques*, permite crear nuevas formas de colaboración entre todo tipo de operadores, y contribuye a facilitar sus relaciones mutuas de forma más eficiente, rápida, segura y fiable. Puede ser de gran utilidad en la gestión de actividades en las que la transparencia y la trazabilidad sean esenciales.

c) La posibilidad de establecer una colaboración global entre diversas personas y entidades, convierte al *Blockchain* en una plataforma fácilmente adaptable a la gestión de proyectos realizados en colaboración, sin importar

que algunas de ellas estén residenciadas en países distintos. Esto es importante en el caso de las entidades que gestionan proyectos de cooperación al desarrollo o reciben donativos de no residentes.

d) Se necesitará la promulgación de la correspondiente cobertura legal, para la aplicación del *Blockchain* a las relaciones entre las fundaciones y las Administraciones Públicas. Especialmente en todo lo relativo a la formalización de las inscripciones registrales y la tramitación de comunicaciones y autorizaciones del Protectorado, y

e) Esta tecnología del *Blockchain* no encaja del todo en la actual normativa sobre protección de datos, lo que hace preciso arbitrar soluciones de futuro que la haga compatible con los principios y derechos en ella regulados, tales como la responsabilidad proactiva de los responsables y encargados del tratamiento, el consentimiento personal expreso y el derecho al olvido.