ALEX PREUKSCHAT
(COORDINADOR)

BLOCKCHAIN:
LA REVOLUCIÓN INDUSTRIAL DE INTERNET

Descubre la tecnología que transformará profundamente internet

Con la colaboración de los principales expertos españoles en Blockchain, entre ellos:
Carlos Kuchkovsky - BBVA
Gonzalo Gómez Lardies - IECISA
Daniel Díez García - everis
Íñigo Molero - OroyFinanzas.com

Índice

Portada

Prólogo. José Luis Várez Benegas

Introducción: ¡Bienvenido a la generación blockchain!

Primera parte. El negocio de la blockchain

1. Los fundamentos de la tecnología blockchain
2. El impacto de la blockchain en las diferentes industrias
3. Modelos de uso sectorial de la blockchain
4. Aplicaciones transversales de la blockchain
5. ¿Cómo invertir en la blockchain?
6. Aspectos legales de los ICO, Smart Contracts y DAO

Segunda parte. La descentralización como modelo de vida

7. Hacktivismo, cypherpunks y el nacimiento de la blockchain
8. La descentralización como modelo de vida

Tercera parte. La tecnología blockchain

9. Criptografía y consenso aplicado a la blockchain
10. Software libre y código abierto en el mundo de las blockchains
11. Seguridad y blockchain
12. Tecnologías blockchain
13. Un mundo de muchas blockchains

Epílogo

Agradecimientos

Autores principales y coordinadores del libro

Notas

Créditos

Prólogo

José Luis Várez Benegas

Querido lector

Si la curiosidad por todo lo que te rodea se ha impuesto a ese irracional temor del ser humano ante los cambios abruptos, estoy seguro de que éste será un libro que agradecerás leer. ¿Por qué? Porque de la misma manera que internet cambió para siempre los modelos de negocio de industrias y empresas centenarias, la blockchain o «cadena de bloques» está dando lugar a un nuevo patrón económico basado en la descentralización de la confianza, donde todos podremos intercambiar bienes y servicios sin necesidad de terceros.

Nuestra intención con este libro es que tú, como lector, adquieras los conocimientos necesarios sobre esta tecnología a fin de que te formes tu propia opinión sobre ella. Para conseguirlo, nos hemos reunido un grupo de profesionales provenientes de muy distintos ámbitos, pero que compartimos un mismo interés por la blockchain y sus infinitas posibilidades. Por ser el más veterano de todos, me ha correspondido el honor de firmar este prólogo, mas no sería del todo sincero si no reconociera que en la amable invitación iba implícita la posibilidad de relatar mi propia experiencia personal y profesional. Y no he podido ni querido negarme.

A lo largo de las siguientes páginas encontrarás información sobre cómo funciona la tecnología blockchain y la forma en la que puede disrumpir en casi todas las industrias, y ello a través de ejemplos, comparaciones y proyectos que son ya una realidad, sin olvidar otras propuestas que, al menos por el momento, se antojan más propias de la ciencia ficción. De este modo podrás tener una visión completa de este nuevo entorno tecnológico que promete transformar nuestras vidas, y de ahí también mi interés en el éxito de este libro, para que nadie pueda decir, digamos dentro de treinta años, que en su momento no dispuso de una herramienta adecuada con la que informarse. Sea este esfuerzo, distribuido y compartido por todos nosotros, nuestra humilde contribución a esta tan necesaria tarea de difusión.

Hace treinta y cinco años, cuando empecé mi carrera profesional, el mundo financiero distaba mucho de ser lo que es hoy. En España no existían gestores de carteras porque tampoco había fondos de inversión en los que invertir. Toda posible inversión se circunscribía a nuestras fronteras y a mercados no referenciados. Pero mi percepción era que más allá había todo un mundo prácticamente inexplorado. Dicho de otro modo, tuve una visión muy clara de lo que iba a acontecer y sólo así, entendiendo y aprendiendo del contexto en el que nos encontrábamos, anticipándonos a los cambios e invirtiendo en el previsible futuro que nosotros mismos dibujábamos, logramos un triunfo extraordinario que compensó con creces nuestros esfuerzos y gratificó, de largo, nuestras percepciones. A nosotros y a nuestros clientes. Surgió así, en 1982, AGEPASA, la tercera gestora de carteras fundada en España.

Nuestra estrategia era tan clara como las sensaciones que nos guiaban. Ahora bien, eso no era suficiente. Debíamos ser capaces también de transmitir a nuestros clientes esas mismas percepciones, convencerles de su validez. Y eso fue lo que hicimos. Entonces nos pareció evidente la nueva senda que se estaba inaugurando y que desembocaría en un mundo globalizado, con Estados Unidos como potencia líder. Aunque todo esto puede parecer hoy muy obvio, lo cierto es que para una amplísima mayoría no lo era tanto entonces.

Pero no nos quedamos ahí, sino que fuimos pioneros también en invertir en los mercados estadounidenses (el NYSE y el NASDAQ), hecho reconocido en su momento por *Barron's*, la primera publicación financiera y de negocios en Estados Unidos. Además, lideramos la canalización de inversión en mercados internacionales a través del desarrollo y comercialización de productos innovadores. Logramos, en definitiva, acercar el mercado internacional a los inversores españoles empleando en la labor a un equipo de doscientos extraordinarios profesionales.

La blockchain tiene un potencial extraordinario y una capacidad de desarrollo y expansión muy por encima de la que he expuesto en mi pequeño relato profesional. Estamos asistiendo al nacimiento de una tecnología que propone nuevas formas de optimizar nuestras relaciones, ahorrar costes administrativos, favorecer cooperaciones sectoriales y todas las posibilidades imaginables. Eso sí, todas estas aplicaciones deberán sustentarse en la seguridad informática y jurídica que se irán articulando con el paso del tiempo.

Hoy, más de tres décadas después de iniciar mi aventura profesional, percibo esa misma sensación y, como entonces, mi actuación no ha de ser diferente. En 2016 fundé BlockLift, un vehículo destinado a explorar oportunidades de negocio y apoyar a otras empresas a la hora de familiarizarse con la tecnología blockchain. Y, como hice entonces, he vuelto a rodearme de expertos en el sector para aplicar la misma estrategia exitosa que logró transformar AGEPASA en el grupo Banco Inversión, con una red de veinte oficinas propias distribuidas por toda España. También hemos sido promotores de la creación en el seno de la Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales (AMETIC) de la primera Comisión Blockchain, dedicada a la divulgación de las oportunidades que esta tecnología va a suponer para las empresas españolas.

Nuestros esfuerzos iniciales se concentran en hacer pedagogía sobre esta nueva tecnología y en suscitar el interés por ella en todas las capas de la población. La blockchain está ahí, accesible a todos y en un mundo donde españoles, estadounidenses, suizos, alemanes, rusos y chinos podemos competir y cooperar en igualdad de condiciones. La única condición necesaria para alcanzar el éxito es un ecosistema propicio en el que desarrollar el talento, el ingenio y el esfuerzo.

¡Bienvenidos a la era blockchain!

Introducción

¡Bienvenido a la generación blockchain!

Álex Preukschat e Íñigo Molero Manglano

Desde que en el año 2009 surgiera la blockchain,[1] el interés por esta tecnología no ha parado de aumentar. Lo demuestra el hecho de que empresas, emprendedores y Gobiernos de todo el mundo estén realizando inversiones millonarias para desarrollarla y tomar una posición privilegiada en la que será la próxima revolución industrial: el internet del valor. Mas aún, estamos entrando en una fase nueva: la de imaginar las posibilidades y los distintos modelos de uso que finalmente adoptará esta tecnología. Y es que el único límite que conoce la blockchain es la propia imaginación del ser humano. Por eso, se hace necesario prever las oportunidades y amenazas que supone su aplicación, ya sea en industrias o en la vida cotidiana. Es lo que hemos intentado con este libro. Nuestro propósito principal al escribirlo es el de compartir contigo, lector, nuestros conocimientos sobre la blockchain, pero con la íntima aspiración de que seas tú mismo quien se forje su propia opinión. Igualmente, nos gustaría pensar que estas páginas ayudarán a que el mundo de habla hispana se convierta en un referente en el desarrollo de esta novedosa tecnología.

El libro está estructurado para transmitir todo el potencial de la blockchain de una forma accesible y cercana. Así, inicialmente exponemos algunos fundamentos que te ayudarán a entender en toda su amplitud el potencial de la blockchain en diferentes industrias y sectores, incluidos modelos de usos actuales que invitan a soñar e imaginar el futuro del internet del valor, que no es lo mismo que el internet de la información. Si éste es el internet que conocemos todos, el que permite la libre circulación en todo el planeta de la información, propiciando la creación de infinidad de nuevos modelos de negocio, el segundo es una herramienta nueva que sirve para compartir y gestionar el valor de activos o bienes digitales sin la necesidad de depender de una entidad central de confianza que centralice el proceso. Sin duda, tratar de imaginar lo que nos deparará este tipo de internet es una labor compleja, tanto como lo habría sido para alguien que escribiera en 1995 una elucubración sobre el desarrollo futuro

de la red. Nosotros no aspiramos a tener una bola de cristal, pero sí a que algunas de las ideas expuestas te ayuden a vislumbrar la importancia y las implicaciones de esta tecnología a nivel mundial.

Una vez asimiladas las implicaciones en industrias y sectores, así como sus aplicaciones transversales, entenderemos una de las cuestiones más novedosas de esta tecnología: el auge de la economía de protocolos de las blockchains públicas y cómo se podría generar un nuevo modelo de inversión que altere la actual distribución del valor, rehaciendo industrias enteras. En realidad, esta nueva economía de los protocolos es anterior al nacimiento de la criptomoneda digital, el bitcoin, y de la propia blockchain. Su origen se halla en el movimiento de descentralización basado en la tecnología que surgió en la década de los setenta con la criptografía y se dinamizó en los años noventa con los cypherpunks. Estos antecedentes serán desarrollados en la sección dedicada a los aspectos filosóficos de la blockchain.

A partir de aquí confiamos en que el lector se anime a descubrir las entrañas técnicas y los procesos de los que se compone la blockchain. Podrá hacerlo en un capítulo en el que nos hemos esforzado en transmitir de forma comprensible conceptos tan fundamentales en este ámbito como «criptografía», «código abierto», «seguridad» y tipos de blockchains. Para ello, hemos reunido a algunas de las personas que más saben al respecto para que compartan con nosotros sus conocimientos y experiencias.

Los países líderes del mundo apuestan por la blockchain

Es importante que desde España y Latinoamérica participemos en este movimiento de la blockchain, pues sólo así podremos situarnos a la altura de los principales núcleos de innovación del mundo, como Londres, Zúrich, San Francisco, Nueva York o Singapur, ciudades todas ellas que ya se han posicionado de forma muy activa —a nivel corporativo, gubernamental y emprendedor— en el internet del valor.

Los políticos británicos, por ejemplo, han sido de los primeros en entender todo el potencial de esta nueva industria, de ahí que el Reino Unido esté subvencionando con 15 millones de libras esterlinas proyectos sustentados en la

blockchain. De este modo, fomentando nuevas formas de negocio, el Gobierno lo que ha conseguido es asegurar el actual estatus de Londres como referencia mundial en la gestión de servicios financieros.

Suiza es otro de los países que mejor están actuando en este sector. Cerca de Zúrich se ha organizado un ecosistema perfecto para inversiones de tecnología blockchain. Este Crypto Valley, como se lo conoce popularmente, cuenta con leyes favorables que proporcionan seguridad jurídica a los emprendedores, una condición esta, básica para atraer el talento dondequiera que éste se halle. A ello hay que sumar una política de bajos impuestos que incentiva las inversiones.

Desde Wall Street hasta Silicon Valley, en Estados Unidos se está también invirtiendo un capital importante para impulsar esta tecnología. Las empresas e inversores de Silicon Valley apuestan sobre todo por las blockchains públicas, como Bitcoin o Ethereum, con la esperanza de triunfar tal y como lo hicieron años antes con el internet de la información. En cambio, en Wall Street, y con el fin de contrarrestar la amenaza que representan las blockchains públicas, se trabaja sobre todo con blockchains privadas, en las que un modelo de negocio regulado tiene una mejor cabida.

En Singapur, las administraciones públicas, pero también las empresas privadas, los académicos y los desarrolladores, han aunado esfuerzos para impulsar esta tecnología. La recompensa a esta coordinación de distintos sectores sociales ha sido la fundación del centro de innovación IBM de blockchain, con sede en esta ciudad-Estado asiática. Singapur es consciente de su privilegiada posición geopolítica y su inversión en la tecnología blockchain revela su intención de seguir formando parte de los países líderes del mundo en este siglo XXI.

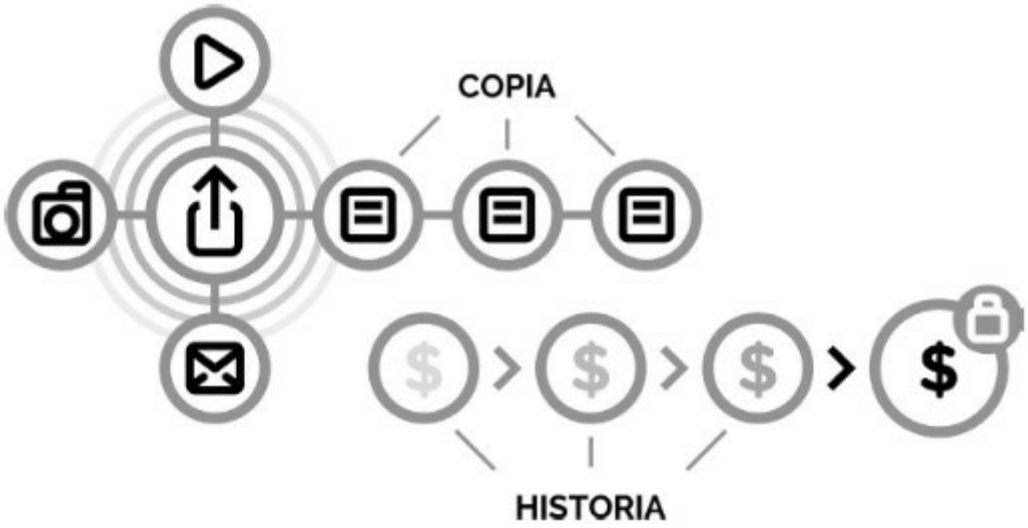
Del internet de la información al internet del valor

La irrupción del internet de la información ha cambiado radicalmente nuestras vidas. Sólo hay que ver el impacto generado por empresas punteras en este ámbito, como Google, Facebook o Amazon, presentes en el día a día de todos nosotros. Todas ellas son la demostración de que el internet de la información

ha creado oportunidades para fundar industrias y modelos de negocio en nuevos sectores de la economía, cambiando de paso dinámicas históricas en industrias ya asentadas.

Otro tanto puede suceder con el internet del valor, una expresión que define el próximo paso en la evolución natural de la red y que sólo ha sido posible a partir del descubrimiento de la tecnología blockchain. Gracias a ésta, este nuevo concepto de internet permite compartir valor (como títulos, registros, certificaciones, archivos o canciones) de una forma digital y descentralizada, sin necesidad de una entidad central de confianza que imponga su criterio a los participantes. Esa capacidad es lo que convierte a la tecnología blockchain en algo tan apasionante y que puede revolucionar nuestra forma de entender el mundo. Tanto, que aquellas industrias y modelos de negocio que no se adapten a los cambios acabarán sucumbiendo.

El internet de la información y el internet del valor.



El internet del valor como salto tecnológico y social

Si una cosa nos enseña la historia es que tecnologías en un primer momento disruptivas han sido, más pronto que tarde, completamente aceptadas e incorporadas a todas las facetas de nuestra vida. Fue el caso de la irrupción del ordenador personal hacia 1975: en apenas dieciséis años su uso estaba generalizado entre la población, de tal modo que cambió nuestra forma de trabajar y relacionarnos los unos con los otros. Otro tanto pasó con los teléfonos móviles: desde su aparición en 1983 tardaron trece años en experimentar una expansión a nivel masivo. Hoy puede decirse, sin temor a exageración, que

existen más móviles operativos que habitantes en este planeta nuestro. Mas la revolución de las revoluciones ha sido la popularización de internet. Si bien esta tecnología empezó a desarrollarse en la década de los sesenta, fue en la de los noventa cuando comenzó a introducirse en los hogares. Desde ese momento, bastaron siete años para que se convirtiera en una herramienta insustituible, de tal modo que si de un día para otro se apagara, el mundo entero se vería envuelto en un colapso difícil de imaginar. Todas estas tecnologías las hemos adoptado en nuestra vida cotidiana. Y lo mismo las empresas, que han recurrido a ellas para desarrollar con mayor eficiencia su modelo de negocio.

Un recorrido similar al de los ordenadores, los teléfonos móviles e internet es el que puede esperarse de la blockchain. Cuando hizo su aparición en escena en 2009 no faltaron sus detractores, gente que afirmaba que esta tecnología no podía tener utilidad práctica alguna, al menos dentro de la legalidad. Se equivocaban: en menos de una década de vida, la blockchain ha demostrado que está aquí para quedarse, aunque nadie pueda afirmar con rotundidad la forma final que adoptará. Es más, hoy nadie duda de que si internet supuso en su momento una revolución en el acceso y difusión de la información, la blockchain representa una revolución en la transmisión y valor de datos en ese mismo internet. En la actualidad, el debate gira en torno a qué forma adoptará y cuándo. Y una cosa está clara: los primeros que entendieron todo el potencial de la blockchain parten con una ventaja competitiva sobre el resto, pues no se quedaron en la teoría, sino que de inmediato se pusieron manos a la obra para concretar sus posibles usos y trabajar en su desarrollo.

PRIMERA PARTE

El negocio de la blockchain

Capítulo 1

Los fundamentos de la tecnología blockchain

Álex Preukschat

Aunque generalmente hablamos de blockchain, lo cierto es que este concepto como tal no existe. O al menos no a secas, sino acompañado siempre de un adjetivo, de modo que podamos diferenciar entre «blockchains públicas», «blockchains privadas» o, incluso, «blockchains híbridas». No obstante, en general se puede hablar de una tecnología que ha llegado para quedarse y, más aún, para definir lo que será el mundo del futuro. Gracias a ella, el actual internet de la información alcanzará un nuevo paso evolutivo, que ya se ha dado en llamar internet del valor.

El consenso, la clave de la blockchain

Una blockchain no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. Otro elemento muy importante a tener en cuenta en ella es que, por definición, se trata de un sistema que permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos. El consenso es precisamente la clave de un sistema blockchain porque es el fundamento que permite que todos los participantes en el mismo puedan confiar en la información que se encuentra grabada en él. Se trata de un aspecto con un potencial increíble para transformar una infinidad de sectores clave de la industria y no menos de la sociedad en la que vivimos, de tal modo que podría llegar a cambiar incluso nuestra forma de entender el mundo.

Desde un punto de vista técnico, ese sistema basado en la confianza y el consenso se construye a partir de una red global de ordenadores que gestionan una gigantesca base de datos. Ésta puede estar abierta a la participación de cualquiera que lo desee (hablamos entonces de una «blockchain pública») o

bien limitada a sólo algunos participantes (caso de la «blockchain privada»), aunque siempre sin la necesidad de una entidad central que supervise o valide los procesos que se lleven a cabo.

La primera de todas las blockchains que han existido fue la blockchain pública de Bitcoin, lanzada en enero de 2009. En su funcionamiento juegan un papel importante términos como «minería», inspirado en la minería del oro y referido al proceso computacional necesario que opera para asegurar su red, la llamada «Prueba de Trabajo» (*Proof of Work*, en inglés, PoW). No obstante, para hacerse una idea del impacto que podría tener la blockchain en el mundo no es imprescindible entender desde un primer momento estos conceptos, en los que ya habrá ocasión de profundizar en los capítulos dedicados a criptografía, consenso y tecnología. En ellos podrás ver que no todas las blockchains se basan en la misma operativa y que incluso hay algunos proyectos que, a pesar de denominarse «blockchain», quizás no lo sean.

Los elementos básicos de la blockchain

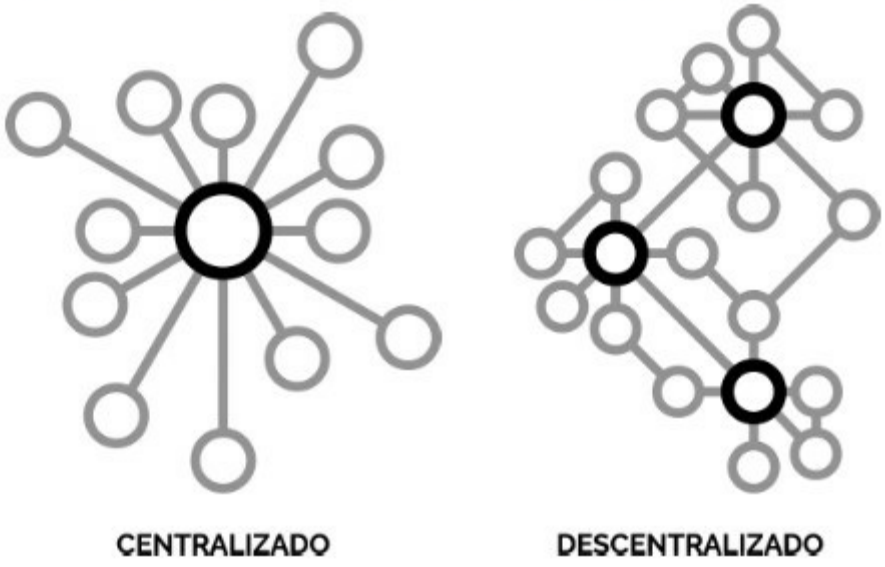
Para entender el alcance de la tecnología blockchain hay que conocer los elementos básicos de que se compone. Son los siguientes:

- **Un nodo:** puede ser un ordenador personal o, según la complejidad de la red, una megacomputadora. Con independencia de la capacidad de cómputo, todos los nodos han de poseer el mismo software/protocolo para comunicarse entre sí. De otro modo no podrán conectarse ni formar parte de la red de una blockchain, sea ésta pública, privada o híbrida. Si en una blockchain pública estos nodos no tienen por qué identificarse, en una blockchain privada los nodos se conocen entre sí, pudiendo también ser iguales entre ellos.
- **Un protocolo estándar:** en forma de software informático para que una red de ordenadores (nodos) pueda comunicarse entre sí. Existen protocolos muy conocidos, como el TCP/IP para internet o el SMPT para el intercambio de correos electrónicos. El protocolo de una blockchain funciona de la misma forma: otorga un estándar común para definir la comunicación entre los ordenadores participantes en la red.

- **Una red entre pares o P2P (Peer-to-Peer, en inglés):** se trata de una red de nodos conectados directamente en una misma red. Un ejemplo muy conocido de red P2P es BitTorrent.
- **Un sistema descentralizado:** a diferencia de un sistema centralizado, donde toda la información está controlada por una única entidad, aquí son todos los ordenadores conectados los que controlan la red porque todos son iguales entre sí; es decir, no hay una jerarquía entre los nodos, al menos en una blockchain pública. En una privada sí puede haber jerarquía.

De lo dicho se desprende que una blockchain es un conjunto de ordenadores (o servidores) llamados «nodos» que, conectados en red, utilizan un mismo sistema de comunicación (el protocolo) con el objetivo de validar y almacenar la misma información registrada en una red P2P. Podríamos decir que ésta sería la estructura «física», como lo es la carrocería en un coche… Pero ¿y el motor? El motor de la blockchain es la suma de todos esos elementos que logran que la información recogida no pueda modificarse porque complejos algoritmos criptográficos, sumados a la propia capacidad colectiva de la red, contribuyen a asegurar la irreversibilidad de la información.

Modelo de red centralizada y de red descentralizada.



Las claves de la tecnología blockchain

Una blockchain se compone de tres partes que, combinadas e integradas, cumplen un propósito determinado y fundamental. Son éstas:

- **La criptografía:** por tal entendemos un procedimiento que, utilizando un

algoritmo con clave (clave de cifrado), transforma un mensaje sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo empleado. En la blockchain, la criptografía tiene la responsabilidad de proveer un mecanismo infalible para la codificación segura de las reglas del protocolo que rigen el sistema. Es también fundamental para evitar la manipulación, hurto o introducción errónea de información en la cadena de bloques, así como la responsable de generar firmas e identidades digitales encriptadas.

- **La cadena de bloques o blockchain:** es la base de datos diseñada para el almacenamiento de los registros realizados por los usuarios. Todas las blockchains han de actuar bajo las mismas reglas o protocolo para dar validez al bloque —y a la información recogida— e incorporarlo a la cadena de bloques. Una vez realizada esta tarea, la cadena continuará con la emisión del siguiente bloque, permaneciendo inalterable la información registrada a través de la criptografía. Esta forma de obrar elimina la necesidad de un tercer ente de confianza.
- **Un consenso:** se trata de una parte imprescindible entre los usuarios de la blockchain. Este consenso se sustenta en un protocolo común que verifica y confirma las transacciones realizadas, y asegura la irreversibilidad de las mismas. De igual modo, este consenso debe proporcionar a todos los usuarios una copia inalterable y actualizada de las operaciones realizadas en la blockchain.

Independientemente de si se opta por una cadena de bloques pública o privada, la combinación de estos tres elementos dentro del protocolo/software otorgan ese sello de calidad que certifica que es un motor blockchain.

Las blockchains públicas versus privadas

Como se ha dicho, la blockchain se puede dividir en dos grandes grupos: públicas y privadas. Siguiendo con nuestro ejemplo del coche, ambas poseen la misma carrocería y el mismo motor, sólo que ahora pueden optar por complementos diferentes, a gusto del consumidor. Las primeras blockchains fueron diseñadas para ser:

- **Públicas:** cualquier persona sin ser usuario puede acceder y consultar las transacciones realizadas.
- **Abiertas:** cualquier persona puede convertirse en usuario y participar del protocolo común si posee unos mínimos conocimientos técnicos.
- **Descentralizadas:** lo son en cuanto que no existe un usuario que tenga más poder que otro en la red y todos los nodos son iguales entre sí.
- **Pseudoanónimas:** los propietarios de transacciones no son identificables personalmente, pero sus direcciones sí son rastreables debido a su carácter público. Por eso, la mayoría de blockchains públicas no pueden ser anónimas, excepto aquellas expresamente diseñadas para ser anónimas.

Por definición, una blockchain pública es una red descentralizada de ordenadores que utilizan un protocolo común asumido por todos los usuarios y que permite a éstos registrar transacciones en el libro mayor (*ledger*, en inglés) de la base de datos. Esas anotaciones son inalterables, si bien los participantes en una blockchain de estas características pueden verificar de forma independiente y por consenso los cambios que se realizan en los registros.

Las unidades de cuenta que se utilizan en las blockchains públicas muchas veces se denominan tokens.[2] Un token no es más que una serie de dígitos que representan un registro dentro de la cadena de bloques. Por ejemplo, una cadena alfanumérica como 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy es un token. Por tanto, un token en una blockchain pública puede ser cualquier cadena alfanumérica que represente un registro en la base de datos descentralizada y que sea aceptada, por consenso, dentro de esa misma blockchain.

Características de la blockchain privada

Ahora bien, la propia tecnología blockchain ofrece la posibilidad de establecer una cadena de bloques con otras características distintas. Así que, de la misma forma, también puede construirse una blockchain privada, cerrada y con participantes identificados. O una privada, abierta y anónima, o una híbrida por asumir características propias de las blockchains públicas y privadas…

Uno de los argumentos esgrimidos por el sector financiero y otros sectores regulados para el desarrollo de las blockchains privadas ha sido la imposibilidad de compartir, por razones regulatorias o de confidencialidad, sus bases de datos de forma abierta. Por tanto, estas blockchains privadas son:

- **Privadas:** porque no todos los datos inscritos en la blockchain tienen difusión pública y sólo los participantes o usuarios pueden acceder y consultar todas o algunas de las transacciones realizadas.
- **Cerradas:** sólo las personas o entidades invitadas a participar adquieren la condición de usuarios o registradores de las transacciones. En este sentido, el protocolo predeterminado podrá incluir distintos niveles de acceso a los usuarios, de modo que unos puedan tener la capacidad de registrar información y otros tener vetada esta opción. El diseño va siempre en función de los fines perseguidos.
- **Distribuidas:** el número de nodos de los que se componga la blockchain privada puede estar limitado al número de participantes o a cierto número de ellos. En cualquier caso, todos los nodos se conocen. La fortaleza de una blockchain se basa en gran medida en la cantidad de los nodos que la protegen y en los incentivos que éstos puedan recibir por cumplir este papel. A mayor número de nodos operativos, menor es la posibilidad de sufrir ataques. Pero, a diferencia de las blockchains públicas, donde el mantenimiento de los nodos depende de la voluntad de los usuarios, en las privadas son los participantes quienes se comprometen a mantener la estabilidad del sistema. Esto significa que una blockchain privada no está sujeta, por así decirlo, a las veleidades que puede sufrir una cadena pública, en la cual es sumamente importante definir correctamente medidas que trabajen a favor de su propia protección.
- **Anónimas:** una blockchain privada puede establecer el nivel de anonimato que quiera para realizar o proteger transacciones. Los usuarios que registran anotaciones pueden estar o no perfectamente identificados.

Los participantes en una blockchain privada, es decir, aquellos que hayan obtenido la condición de usuarios, están sujetos a un protocolo predeterminado que los podrá capacitar, según se establezca, para participar en el registro de las anotaciones y/o verificar los cambios introducidos en la cadena. En este sentido,

una blockchain privada podría estar más centralizada y el número de nodos que componen la red podría limitarse al número de usuarios necesarios establecido por los promotores. Hablaríamos entonces de una base de datos conjunta gestionada por ese grupo de usuarios, en la que —y de la misma forma que en una blockchain pública— las anotaciones realizadas serán inalterables.

En la tecnología blockchain privada también se habla muchas veces de libro mayor en referencia a un registro global de transacciones, tal y como se conoce en la contabilidad tradicional. Tanto es así que las iniciativas de blockchains privadas se denominan con frecuencia en inglés *Distributed Ledger Technology* (DLT), lo que en castellano equivale a decir Tecnología de Libro Mayor Distribuido. Por otro lado, la blockchain privada es distribuida, en el sentido de que es una base de datos repartida en varios nodos, mientras que la pública es descentralizada, porque en ella no se controla quién participa en la misma.

De forma coloquial se puede decir que una blockchain es pública si cualquier usuario puede participar en ella libremente, de ahí que se la llame también «blockchain sin permiso» (*permisionless*, en inglés). En cambio, en una privada la posibilidad de participar no está al alcance de todo el mundo, aunque el código utilizado sea público: la persona debe ser invitada a participar, razón por la cual en ocasiones se la denomina «blockchain con permiso» (*permissioned*, en inglés). Con el tiempo se consolidarán multitud de blockchains con características distintas para cumplir con diferentes fines. Unas serán públicas, otras privadas[3] y no faltarán tampoco las híbridas, dependiendo del modelo de uso para el que hayan sido concebidas.

Capítulo 2

El impacto de la blockchain en las diferentes industrias

El internet de la información empezó a tomar forma dentro de los sectores militar y académico, y desde ellos se expandió al resto de industrias. En el internet del valor ha sido el sector financiero el primero en tomar la iniciativa. Pero, como en el caso anterior, la aplicación de esta tecnología no será exclusiva de un único sector, pues cada vez son más las industrias que exploran todo su potencial. A lo largo de este capítulo presentaremos algunas de ellas.

Ejemplos de industrias dentro del internet del valor.

Banca y blockchain, ¿pioneros por necesidad?

Daniel Díez García y Gonzalo Gómez Lardies

Desde la crisis financiera de 2008, el sector bancario experimenta dificultades para mantener los niveles de rentabilidad anteriores a esa fecha. No es extraño así que busque revertir esta tendencia apostando por una fuerte inversión en la innovación representada por la tecnología blockchain. Los bancos e instituciones financieras apuestan, sobre todo, por las blockchains privadas para desarrollar modelos de uso. Frente a ellas, se sitúan las grandes empresas de capital riesgo de Silicon Valley y los gigantes de internet, que prefieren las blockchains públicas para introducirse en el mundo Fintech e Insurtech (empresas de tecnología centradas en la industria del seguro).

Bitcoin: el nacimiento de la banca descentralizada

En la década de los noventa, un grupo de personas conocidas como cypherpunks decidió aprovechar todo el potencial de la infraestructura de internet y crear un sistema financiero abierto, sin entes centrales, que garantizara el anonimato, el control de la oferta monetaria y, a la vez, fuera totalmente transparente. El resultado llegó en 2008 con la creación de una criptodivisa: bitcoin.[4] Con ella se inició una primera ola de descentralización en campos tan importantes como son los pagos, las transferencias internacionales y las remesas. Pero la importancia del bitcoin va más allá de todo esto: mostró que ya no era necesario contar con un banco o ningún tipo de tercero de confianza para llevar a cabo gran parte de las labores que tradicionalmente ha desempeñado la banca. Fue, por tanto, el primer caso de uso de la tecnología blockchain.

La blockchain permite simplificar, en gran medida, pagos internacionales al eliminar potencialmente la necesidad de cámaras de compensación y crear un nuevo estándar de interoperabilidad entre entidades financieras. Añadiendo sistemas desintermediados, transparentes y automatizados, desaparecen los riesgos operativos, ya que no hay posibilidad de incumplir las condiciones de los contratos digitales inteligentes que hayan firmado las diferentes partes

involucradas. La consecuencia de todo esto es que se reduce considerablemente la necesidad de disponer de circulante o líneas de crédito, y se da pie a ofrecer márgenes mucho más ajustados en los servicios (por ejemplo, préstamos), eliminándose de paso la necesidad de confianza entre las diferentes partes.

Banca: ¿cuál podría ser su futuro?

Existen diversas razones por las cuales el sector bancario se encuentra en plena transformación. No se trata de un cambio exclusivamente tecnológico, sino también cultural y regulatorio, debido a nuevos hábitos de vida y consumo de servicios que afectan también a la relación entre empresa y cliente. Nos movemos en un paradigma en el que el objetivo ya no es vender servicios a los clientes como tal, sino acompañarlos a lo largo de sus vidas para satisfacer sus deseos y necesidades de la forma más líquida posible. Entre los motivos que han acelerado este cambio cultural y operativo destacan la rentabilidad de la banca, su regulación, los nuevos competidores que le han surgido y la distribución de capacidades y cambio de modelo comercial. A continuación explicamos cada uno de ellos en detalle.

La rentabilidad de la banca

Las principales líneas de negocio de la banca son el crédito, en primer lugar, y la venta de productos financieros, en segundo. En el primer caso, la banca había contado históricamente con un amplio margen entre los intereses que se pagaban a los depositantes y los que se cobraban a los solicitantes de préstamos. Asimismo, debido a la asimetría de información entre las instituciones financieras y los clientes, la opacidad y falta de información para estos últimos permitía que las primeras minusvalorasen riesgos en la venta de productos financieros de baja calidad, calificándolos, en ocasiones, como depósitos o productos de renta fija cuando en realidad eran de renta variable. Eso es lo que pasó en el conocido caso del fraude de las preferentes en España.

En los últimos años, las políticas monetarias expansivas y las bajadas de los tipos de interés han afectado negativamente a la rentabilidad bancaria. Debido al exceso de liquidez, los tipos de interés de los préstamos siguen cayendo, mientras que los de los depósitos a cuenta mantienen un suelo del 0%. En esta situación el margen de intermediación con el que cuenta la banca se hace cada

vez más estrecho, por lo que las entidades se ven obligadas a realizar el cobro de comisiones de forma más directa. Lo que los clientes pagaban antiguamente sin ser conscientes de ello (debido a ese mayor margen de intermediación), ahora deben pagarlo de forma explícita con comisiones por retirada de efectivo, transferencias o mantenimiento de cuenta, entre otros servicios complementarios. La consecuencia de esto no es otra que la pérdida de confianza por parte de los clientes y el empeoramiento de la experiencia como usuario.

Este estrecho margen de intermediación se ha traducido en dos estrategias comerciales para intentar mejorar la operativa: por un lado, la reducción de los gastos de explotación mediante recortes de plantilla, cierre de oficinas, fusiones e inversiones en tecnología; por otro, y muy especialmente, la reorientación del modelo de negocio a actividades que generen ingresos distintos al cobro de intereses y aporten nuevas capas de valor sobre la operativa existente.

Desde el prisma de la blockchain se puede optimizar en gran medida la operativa reduciendo notablemente los costes. Pero es en la segunda vía, en la de la reorientación, donde encontramos un valor diferencial para esta tecnología gracias a la generación de nuevas plataformas y modelos de negocio en los que la flexibilidad, la transparencia, la interoperabilidad, la automatización y las experiencias del usuario cobran un papel fundamental.

La regulación de la banca

Existen dos iniciativas legales llamadas a cambiar radicalmente el ecosistema de servicios bancarios y la relación entre entidad y cliente: la MiFID II (Markets in Financial Instruments Directive II) y la PSD2 (Directive on Payment Services 2).

La primera de ellas, la MiFID II, con entrada en vigor en enero del año 2018, tiene como objetivo transformar el modelo de asesoramiento y venta de productos financieros a clientes, aportando más transparencia a un mercado tradicionalmente opaco y evitando malas prácticas como la venta en masa de productos «genéricos» cuyos riesgos se acostumbraba a minusvalorar.

Con la MiFID II, los asesores financieros tienen opción de elegir entre declararse independientes (lo que les impide cobrar el porcentaje de los productos de las gestoras que venden) o dependientes, y vender entonces

aquellos productos de mayor comisión. La MiFID II permite también que donde antes un inversor pensaba que el asesoramiento era gratuito, ahora identifique perfectamente toda la relación de costes. En definitiva, se pasa a un modelo en el que el objetivo del asesoramiento no consiste en cumplir con los objetivos del banco, sino con los del cliente.

En lo que respecta a la normativa PSD2, supone una revolución en la naturaleza del modelo de negocio de la banca aplicada al ámbito de los pagos, pues con ella se pasa de un modelo de negocio tradicional a otro con un carácter mucho más abierto, en el que la banca tiene que exponer sus «entrañas» a la comunidad abierta de desarrolladores y nuevas Fintechs mediante la implementación de interfaces de programación de aplicaciones (en inglés, Application Programming Interface, API). Estas API pueden dirigirse a dos tipos de proveedores: los que puedan iniciar pagos desde cualquier plataforma online, y aquellos otros que ya sean conocidos como agregadores de información financiera y permitan acceder a información del cliente y ofrecerle servicios de valor añadido.

Si la MiFID II tiene como objetivo velar por la protección al consumidor, la PSD2 persigue generar oferta para los consumidores y fomentar la competencia. Es alineándose con esta nueva normativa como la blockchain puede ofrecer un valor diferencial a las empresas que les permita alcanzar nuevos estándares de transparencia y apertura de modelos de negocio. Por todo lo expuesto, podemos convenir que la regulación avanza en la línea de ser más una gran aliada que una barrera en lo que a la adopción de esta tecnología se refiere.

La blockchain posibilita la transición a un mundo transparente, abierto, seguro y altamente interconectado, en el cual los clientes tienen pleno control sobre su identidad digital y conocimiento de los activos y servicios que contratan. Aquellos agentes que consigan dar un mayor valor a sus productos serán quienes obtengan una principal ventaja competitiva y unos mayores rendimientos económicos.

Nuevos competidores de la banca

Tanto la regulación como las nuevas tecnologías han propiciado la aparición de nuevos competidores, capaces de desintermediar crédito, pagos y envíos de remesas entre otros mercados. Estos competidores tiempo atrás estaban caracterizados por la oferta de nuevas soluciones, que si bien proveían de un gran valor a los clientes con magníficas experiencias de usuario, no cumplían con la regulación pertinente.

Actualmente, y más allá de la incursión de gigantes tecnológicos como las GAFA (Google, Apple, Facebook y Amazon), contamos con un amplio espectro de empresas que, frente a la incapacidad de innovar de las grandes firmas (en el caso de la banca, en numerosos casos resulta más eficiente crear otro banco desde cero que innovar sobre el original), se muestran flexibles, ágiles y completamente volcadas sobre el cliente. Se trata de una clara propuesta de valor que llega a ofrecer incluso servicios bancarios a usuarios de países desbancarizados (recordemos que el 38 % de la población mundial carece de una cuenta bancaria). En una era digital en la que priman los servicios vivos y las expectativas líquidas, la propia experiencia del usuario será la principal ventaja competitiva que determinará el crecimiento y la supervivencia de las empresas, quedando la propia naturaleza de cada modelo de negocio relegada a un segundo plano.

Nos encontramos, pues, en una etapa en la que el foco de las empresas ha pasado del plano de la competición directa (aquellos que venden el mismo producto) a situarse en el plano experiencial (aquellos competidores que ofrecen experiencias que sustituyen a las nuestras) para, finalmente, centrarse en el plano perceptual (competidores que pueden cambiar los hábitos de consumo y expectativas de nuestros clientes).

La conclusión es clara: necesitamos empresas que acompañen a sus clientes y los provean del máximo valor en tiempo real y en cualquier sitio, conociendo e incluso anticipándose a sus demandas, deseos y necesidades.

Por ello, el siguiente reto de la banca pasa por ofrecer experiencias de usuario excepcionales y obtener un rendimiento de la información que las entidades están ofreciendo a terceros, yendo más allá de una API limitada que

cumpla con la regulación. En suma, se convertirá en un proveedor de información de cuentas abierto que trabaje con comunidades abiertas de desarrolladores y compita directamente con las GAFA y Fintechs.

Distribución de capacidades y cambio de modelo comercial (sucursal digital)

Tradicionalmente, el asesor comercial y el cliente concertaban una cita y se encontraban en persona, estableciéndose entre ellos una relación de larga duración basada en la confianza. El conocimiento del cliente posibilitaba unas soluciones personalizadas. Esto era un activo mucho más valioso que todos los registros que pudiera haber en la base de datos de la entidad.

En la actualidad, la crisis de reputación del sector y el auge de las nuevas tecnologías está propiciando que el cliente sustituya la figura del asesor comercial por diferentes proveedores de información y servicios que pasan a asumir ese rol. Debido al grado de disponibilidad de información sobre nuestros gustos, situación personal y preferencias, las oficinas de siempre no consiguen ya ofrecer una experiencia de usuario equivalente a la de otros competidores perceptuales. Dejan, por tanto, de ser rentables. Hay que redifinirlas, y lo mismo puede decirse de la propia figura del asesor comercial. Gracias a las nuevas herramientas tecnológicas disponibles, esta figura en concreto podría incluso digitalizarse, transformarse en una inteligencia artificial.

Para llevar a cabo este cambio al modelo digital se precisa una visión más global, puesto que el análisis de capacidades que ha de llevar al cumplimiento de las necesidades, deseos y demandas de los clientes no debe recaer sobre el equipo comercial, sino sobre toda la organización en su conjunto. Esto significa que la labor comercial deberá ser el último eslabón de un conjunto de elementos que proporcionen al cliente el mejor servicio y experiencia de usuario posibles.

La blockchain: casos de uso en la banca

La blockchain nace para descentralizar la confianza que hemos depositado en las instituciones financieras. En la era digital es necesario que, dada la elevada interconectividad, competencia y automatización de procesos, las empresas tanto tradicionales como de nueva creación modifiquen sus mecanismos para innovar

en base a estándares y modelos de negocio lo más abiertos posibles. Más allá de programar el dinero, la blockchain nos permite programar confianza, propiedad, identidad, activos y contratos, mediante pagos, transacciones, procesos, autentificación, reconciliación e información en tiempo real, y todo con plena transparencia y auditabilidad.

Existen cuatro principales aplicaciones de la blockchain para optimizar el entorno bancario, que más allá del ahorro y simplificación estructural y reducción de costes operativos, permiten la creación de nuevos servicios y modelos de negocio. Estas aplicaciones son: Pagos Globales, Trade Finance, Liquidación de Transacciones y Cumplimentación de la Regulación Automatizada.

Tradicionalmente, ha existido un problema de falta de interoperabilidad entre las diferentes entidades financieras, incluso entre aquellas que pertenecen al mismo grupo, debido a la diferente regulación que se aplica en cada país. En la actualidad existen numerosos proveedores de pagos, el más popular de los cuales es SWIFT, con más de diez mil sociedades financieras formando parte de la cooperativa. La función de SWIFT es la de establecer un estándar de mensajería entre bancos. Para entender en qué consiste, imaginemos que queremos enviar 1.000 euros a un pariente que se encuentra en Estados Unidos: cuando iniciamos la transferencia, el banco emisor genera un mensaje que indica de qué forma vamos a hacer llegar los fondos a ese cliente (fecha, divisas, gastos, a través de qué intermediarios…). Ese mensaje es el SWIFT, la prueba de la realización irrevocable de una transferencia internacional, lo que proporciona una gran seguridad tanto al emisor como al receptor del pago.

La propia naturaleza de SWIFT y la necesidad de un posterior proceso de liquidación entre entidades hace que este tipo de transferencias se lleguen a demorar entre dos y cuatro días, lo que abre la necesidad de establecer líneas de crédito para aquellas empresas que tengan operaciones globales. Si estos pagos fueran instantáneos, desaparecería la necesidad de este tipo de operaciones, reduciéndose en gran medida también el volumen del circulante. Afortunadamente, todo eso ha cambiado hoy gracias a las blockchains, tanto a las públicas como a las privadas. Ambas son ya las dos principales vías para llevar a cabo pagos internacionales.

Las blockchains públicas y su uso en la banca

Las blockchains públicas más populares son Bitcoin y Ethereum. Gracias a ellas, cualquier persona o empresa puede convertirse tanto en usuario como en validador de la red y formar parte como un nodo de la misma. En este tipo de redes, en las que no es necesario ningún tipo de confianza entre las diferentes partes para llegar al consenso sobre el estado y evolución de una serie de factores compartidos (función de una blockchain), cualquier usuario puede enviar dinero sin que importen las fronteras territoriales y, en función de la plataforma y nivel de seguridad elegidos, en un lapso que oscila entre los 15 segundos y los 60 minutos, y con un coste reducido. La principal limitación de estas plataformas es la necesidad de emplear criptomonedas o tokens para transmitir el valor, aspecto este que se explica con más detalle en el apartado de inversión de este libro.

Frente a plataformas consolidadas en un modelo tradicional, como Western Union o Moneygram, las nuevas propuestas aportan un especial valor en países donde no existe una infraestructura financiera sólida y puede que haya fuertes controles de capital e inflación (caso de Venezuela, Argentina, Zimbabue o China), se da un elevado número de población desbancarizada (México) o esa población ha perdido la confianza en su propio sistema financiero (Chipre). Es en estos casos donde las criptomonedas aportan un plus en seguridad a los usuarios en términos de facilidad de uso, imposibilidad de confiscación o control y reserva de valor. En este ámbito existen tres ejemplos de referencia:

- **Abra** (goabra.com): es un servicio de remesas persona a persona. En el caso de que el destinatario no tenga una cuenta de banco (no bancarizada), Abra gestiona una red de personas físicas en muchos países, llamadas *Tellers*, que hacen la función de cajero automático y entregan el dinero al destinatario.
- **BitPesa** (bitpesa.com): se ha especializado en envíos de dinero a y desde África, especialmente en países como Kenia, Nigeria, Tanzania y Uganda. De este modo, un pequeño comerciante puede desarrollar su negocio de importación y/o exportación gracias a una mayor agilidad y un menor coste en el envío de dinero.

- **Circle** (circle.com): es una startup que permite realizar envíos de dinero sin comisiones. Para aquellos envíos que tengan como destino países desbancarizados o con controles de divisas, recurre a criptomonedas.

Las blockchains privadas y su uso en la banca

Una de las plataformas más prometedoras en el ámbito de las blockchains privadas es Ripple (ripple.com). Su especialidad son los pagos internacionales interbancarios, así como el proceso de conversión de divisas. En sí, Ripple es un sistema abierto (cualquiera puede usar Ripple, al igual que Bitcoin o Ethereum), si bien aquellas partes que quieran participar como proveedoras de liquidez para las conversiones de divisas deben estar previamente autorizadas por Ripple. Es, por tanto, un sistema más privado y con un ámbito de confianza más reducido que los públicos descritos anteriormente.

Las transacciones internacionales se completan en tan solo 5 o 10 segundos, y en ellas se hace uso de un proceso de subasta a la baja en el que los diferentes proveedores de liquidez compiten para procesar los pagos. Una vez se produce el *match*, Ripple se encarga del proceso de liquidación entre las dos partes, tarea ejecutada en tiempo real.

Otras soluciones son las que ofrecen R3 (con su producto Corda) o Hyperledger, perteneciente a la Fundación Linux. Ambas trabajan en soluciones para la banca y apuestan por un registro distribuido entre las diferentes entidades del consorcio, lo que les confiere la posibilidad de transferir en tiempo real dinero y otros activos digitales mediante tokens.

Trade Finance en la blockchain

El elevado nivel de burocracia y de procesos manuales de las transacciones tradicionales suman tiempos muertos en los diferentes procesos. Además, siempre queda el miedo de que una de las partes no cumpla con los tiempos de envío y pago, o con las condiciones de calidad. Por suerte, en la actualidad existe una gran oportunidad para digitalizar la comunicación y automatizar procesos en la cadena de suministro.

Más allá de la notable reducción del circulante que aportan los pagos en tiempo real, los contratos inteligentes y el internet de las cosas e identidad digital podrían permitir automatizar la compraventa de mercancía de forma segura, incluyendo todas y cada una de las etapas involucradas en el proceso. Asimismo, gracias a la transparencia, inmutabilidad y trazabilidad características de la blockchain, podríamos conocer y certificar el origen de la mercancía, sin posibilidad de falsificación alguna de la información relativa a la misma. El objetivo es la digitalización de la *Bill of Lading* («conocimiento del embarque»), es decir, el conocimiento que establece la relación contractual entre el cargador, consignatario de la carga y el transportista. Entre las startups que están trabajando en esa línea destacan Fluent, Provenance, Skuchain y Wave.

Cumplimentación de la regulación automatizada

Gracias a la tokenización de identidades y consorcios de identidades digitales será posible que un usuario que se ha dado de alta en una entidad no tenga que aportar de nuevo toda su información personal en el momento de darse de alta en otra de las entidades que pertenezcan a dicho consorcio. Esa cuenta podría crearse con tan sólo una foto de su rostro, limitándose así la cantidad de información cedida y el riesgo de robo y suplantación de identidad.

Este conocimiento de la identidad, sumado a una completa trazabilidad de las operaciones de inicio a fin, permite la monitorización y detección de actividad sospechosa, y propicia también una fácil incorporación de organismos que puedan auditar la información en tiempo real y de ese modo imposibilitar el fraude.

Préstamos en la blockchain

La causa principal por la que individuos y empresas recurren al crédito suministrado por grandes entidades financieras no es otra que la confianza. Ésta, sin embargo, puede convertirse en algo prescindible si se elimina la figura de los intermediarios que arbitran entre ahorradores y solicitantes de crédito. Para ello bastaría con aplicar un software autónomo y los Smart Contracts que garanticen que ambas partes cumplen con sus obligaciones contractuales.

Más allá de la transparencia y de los nuevos modelos de *scoring* (ese sistema automático que, partiendo de una información dada, recomienda la aprobación o no de una operación de financiación), esta desintermediación haría posible que se desarrollen plataformas que permitan un acuerdo entre las diferentes partes, sin ofrecer ellas mismas el préstamo en sí ni retener en ningún momento los fondos, ni siquiera la identidad de los usuarios, pues son ellos mismos quienes la proporcionan para ejecutar acciones mediante su token de identidad. Una de las principales aplicaciones sería el crédito al consumo, donde diferentes individuos o empresas podrían competir mediante subastas a la baja en proporcionar estos fondos, a cambio de unas condiciones transparentes y previamente pactadas.

Las aseguradoras se reinventan

Gonzalo Gómez Lardies y Daniel Díez García

Aunque la banca ha sido la industria que más atención ha prestado a la blockchain, hay otras que no le van a la zaga y que, gracias a esta tecnología, podrían rehacer una gran parte de la operativa y variar el concepto actual de generación de valor. Es el caso de la industria de seguros. Los principales actores de este sector son conscientes de que necesitan aumentar sus márgenes de rentabilidad. Las aseguradoras también saben que en gran medida, para alcanzar ese objetivo, deben adaptar un modelo de negocio tradicional —con escasos cambios en las últimas décadas— a la etapa de desarrollo en la que se encuentra actualmente la sociedad de la información. Además, la aprobación de Solvencia II[5] (Solvency II) y los nuevos baremos de indemnización de accidentes incluidos en el proceso de convergencia del sector asegurador europeo abren nuevas oportunidades, a la par que nuevos retos a los que dar respuesta en un corto espacio de tiempo. Uno de ellos es la aparición de un nuevo tipo de cliente, nativo digital o no, muy exigente y motivado para comparar todos y cada uno de los servicios ofertados, así como las cláusulas incluidas en las pólizas contratadas.

Como consecuencia de todo ello, y al igual que ocurre con la banca, la competencia en el sector asegurador ha crecido exponencialmente. Y se espera que en los próximos años aumente aún más gracias al desarrollo de startups completamente digitales y especializadas (las denominadas Insurtech) que colaborarán y competirán con el sector de seguros establecido. Estas startups utilizan la última tecnología, como el Big Data, el internet de las cosas o la inteligencia cognitiva, para diseñar productos y servicios adaptados a las necesidades del sector. La blockchain es un ingrediente más de este cóctel tecnológico que está transformando el sector de los seguros y sus objetivos de retención y crecimiento de clientela y rentabilidad. De hecho, ya se usa para mejorar tanto la experiencia de usuario como la eficiencia en ramas clave del negocio como la salud o la automoción.

En la actualidad, empresas como la banca o la gran distribución ofrecen también servicios asociados a los seguros. Esto hace que se genere una nueva dinámica de negocio dentro del sector y que la blockchain juegue un papel primordial en ella, pues es la que permite que todos los actores participantes en la cadena de valor (aseguradoras y clientes, agentes y mediadores o técnico y peritos) pueden intercambiar información de manera segura, rápida y constante por medio de una infraestructura abierta, descentralizada, fiable y flexible.

El impacto de la blockchain en las aseguradoras

Uno de los primeros pasos que se han dado en este sector de los seguros ha sido el lanzamiento de un consorcio blockchain por parte de cinco reaseguradoras: Aegon, Allianz, Munich Re, Swiss Re y Zurich.[6] Todas ellas han optado por compartir sinergias e investigar las nuevas posibilidades que ofrece esta tecnología. El resultado ha sido un clúster denominado Blockchain Insurance Industry Initiative-B3i, que funciona como plataforma común en la que poner en valor nuevas ideas, casos de uso y experiencias, con el fin de transformar la forma en la que actualmente se trabaja.

El gran potencial que las empresas aseguradoras han visto en la blockchain se basa inicialmente en la utilización de contratos inteligentes (Smart Contracts), que explicaremos con más detalle en la sección de aplicaciones transversales de este libro. Algunos analistas[7] afirman que el uso de este tipo de contratos será generalizado hacia el año 2020, sobre todo en sectores como la salud, el automóvil, el hogar y los viajes, en los que la comprobación de los casos que debe cumplir la cobertura del contrato puede ser casi inmediata. Con estos contratos inteligentes, las compañías aseguradoras contarán con una auténtica «piedra filosofal» que permitirá que las reacciones en cadena se sucedan, de forma automatizada, en cuanto acontezca un hecho estipulado.

Estos contratos inteligentes podrían incluso permitir a las empresas aseguradoras actuar «de oficio» ante cualquier eventualidad. Por ejemplo, un pasajero que haya adquirido un billete con un seguro de reembolso ante determinadas circunstancias, como la de quedarse en tierra, recibirá, en caso de que eso suceda, el reembolso de la cantidad[8] estipulada de manera directa y sin necesidad de redactar reclamación alguna. El pago de la indemnización se efectúa de manera inmediata porque está asociado a un contrato inteligente. En

este supuesto, el índice de satisfacción del cliente alcanza una cota elevada, lo mismo que su confianza en la compañía. Y todo gracias a la tecnología blockchain. Pero no se trata sólo de fidelizar a los usuarios, sino también de inaugurar nuevos modelos de negocio, pues el sistema permite reducir costes y procedimientos, y da además la posibilidad de pagar el servicio con cualquier divisa válida dentro de las plataformas.

La blockchain, punto de inflexión en el modelo de negocio del sector asegurador

La posibilidad de que todos los actores implicados en la cadena de valor de las aseguradoras dispongan de una red virtual en la que interoperar entre sí permitirá ahorrar costes, además de agilizar la gestión de información entre las partes. Esto redundará en una mejora del servicio y en el consiguiente incremento de la satisfacción de los clientes. A su vez, la fidelidad de éstos abrirá nuevos márgenes de crecimiento a las compañías, lo que repercutirá obviamente en la cuenta de resultados y permitirá que cada empresa aseguradora pueda desviar parte de sus ingresos al departamento de I+D+i, para desarrollar nuevos productos y servicios basados en este tipo de plataformas.

Un aspecto no menos importante es la seguridad, que también se ve incrementada con la tecnología blockchain. El que cada contrato almacenado dentro de la red distribuida tenga asociado un código de almacenamiento en la cadena de bloques y esté encriptado con algoritmos seguros dificultará la posibilidad de que se cometa algún tipo de fraude al hacer más fácil la detección de información falsa que no se corresponda con lo estipulado y codificado en cada contrato. De la misma forma, actualizar los datos de los clientes y de los intermediarios que los atienden en caso de incidencia dejará de ser un proceso largo y engorroso, pues todas las gestiones dispondrán de una plataforma que permitirá la revisión y actualización ágil de cualquier dato nuevo que sea necesario incorporar.

El gran revulsivo de la blockchain será, sin duda, la posibilidad de diseñar productos *ad hoc*, es decir, trajes a medida en función de distintos parámetros y enfocados a satisfacer necesidades puntuales de los clientes.

La blockchain: casos de uso y potenciales aplicaciones

para innovar en el sector asegurador

Una de las entidades que ofrece uno de los ejemplos prácticos más clarificadores sobre las posibilidades que brinda la blockchain es la Fundación Ethereum. Puntera en lo que se refiere a la creación de contratos inteligentes en las blockchains públicas, permite, entre otras cosas, financiar la fabricación y/o venta de un producto vía crowdfunding. Así, mediante la creación de los Smart Contracts podría tomar forma una venta de acciones virtuales o bien subastarse un determinado lote de productos. Se trata, pues, de una nueva manera, fiable, transparente y flexible, de establecer todo el proceso de financiación, compra de acciones o subasta.

Aseguradoras de salud y la blockchain

España cuenta con más de 7 millones de personas que disfrutan de un seguro de salud privado. Gracias a la blockchain y a la implementación de los Smart Contracts,[9] las aseguradoras del ramo de la salud podrán abaratar los costes administrativos al contar con un sistema que pueda proteger los archivos y gestionarlos al mismo tiempo. Igualmente, será posible relacionar automáticamente y de forma descentralizada los datos sobre acuerdos, transacciones y registros médicos, lo que facilitará la comunicación entre pacientes, asegurados, médicos, hospitales y aseguradoras. Otra ventaja de estos contratos, tanto para la empresa aseguradora como para los clientes, es que permitirán combatir el fraude de una manera cien por cien eficaz.

Aseguradoras de coches y la blockchain

Supongamos que un conductor quisiera asegurar su vehículo y que, gracias a la existencia de un sistema blockchain, tuviera la posibilidad de transmitir, de forma anónima y totalmente confidencial, su historial de siniestros para la realización de un estudio. En el caso de que el automóvil[10] estuviera sensorizado —lo que implicaría la combinación de la blockchain con el internet de las cosas —, este informe podría completarse con datos significativos sobre los hábitos de conducción de la persona.

Ese mismo conductor podría transmitir por igual a varias compañías aseguradoras su petición de asegurar su coche. Una vez procesada y analizada la solicitud según los criterios de evaluación de riesgo de la aseguradora, el conductor recibiría varios contratos inteligentes con distintas ofertas. Una vez optara por firmar uno de esos contratos, verificaría su identidad a la aseguradora, demostraría ser propietario del coche, ingresaría el dinero de la póliza y recibiría el certificado y prueba de su seguro.

Hasta hace bien poco, los parámetros de que disponía la compañía aseguradora para formalizar una póliza solían limitarse a la edad del conductor, sus años de experiencia al volante, la marca del vehículo o la potencia del mismo. Cuando la blockchain entre de lleno en el sector asegurador las pólizas no sólo podrán ser mucho más personalizadas, sino que actualizarán dichos parámetros de manera constante y sin la posibilidad de falsear datos pasados. De este modo nos podremos encontrar con seguros cuyas tarifas podrán subir o bajar en función de los kilómetros que haya hecho el conductor durante el mes anterior, de si está al corriente de la ITV o de si ha efectuado las revisiones periódicas que dicta el fabricante. Yendo más allá, en el momento en que los Smart Contract se «crucen» con los coches inteligentes,[11] las compañías de seguros podrán identificar el estado real en todo momento del bien asegurado.

¿Y qué repercusión puede tener en las cuentas de resultados de las aseguradoras la utilización de estos contratos inteligentes en el ramo de los automóviles? Algunos estudios[12] realizados en el Reino Unido indican un ahorro potencial de más de 19.000 millones de euros anuales, y ello sólo por la reducción de trámites. Si esos ahorros se trasladasen en parte a las primas que pagan los asegurados, el beneficio sería doble.

Seguros para agricultores y la blockchain

Supongamos ahora el caso de un agricultor[13] que desee asegurar parte de su cosecha ante el temor de que cualquier temporal acabe con ella. Podría enviar información a las aseguradoras sobre la superficie que desea asegurar y el potencial valor de lo que cultiva en ella. Tras recibir la póliza en función de la información aportada y pagar la prima correspondiente, el agricultor dispondría de un contrato inteligente en el que podría incluirse una cláusula que, para evitar fraudes, le llevara a asumir el compromiso de enviar con cierta periodicidad

fotografías geolocalizadas de la parcela asegurada que permitiesen comprobar el estado de la cosecha. La aseguradora podría también utilizar los servicios de una empresa de drones para certificar la información de forma visual e independiente.

En caso de que se produjese un siniestro que exigiera el pago de la suma asegurada, podría comprobarse automáticamente la veracidad de la imagen enviada por el agricultor en el momento del hecho y compararla con imágenes satelitales o de un servicio de drones de la citada área. Efectuada esta comprobación, se procedería a pagar automáticamente la cantidad asegurada al agricultor.

Las aseguradoras del futuro serán expertas en la blockchain

Un aspecto donde prácticamente coinciden todas las aseguradoras es que la blockchain permitirá la creación de nuevos modelos de seguro, incluso nuevos ramos, donde la personalización, tanto de coberturas como de costes para el usuario final, serán imprescindibles.

De la capacidad que tengan las entidades aseguradoras para digitalizarse y asumir riesgos para crear nuevos productos basados en blockchain, tras un proceso de aprendizaje basado en el ensayo y error, dependerá la evolución del sector hasta la próxima década.

Más información sobre el impacto de la blockchain para las aseguradoras en <libroblockchain.com/aseguradoras/>.

Telecomunicaciones: de la revolución de datos a la revolución blockchain

Christoph Steck y Eusebio Felguera Garrido

Cualquier industria que utilice bases de datos centralizadas que sean alimentadas por diferentes fuentes es susceptible de verse afectada por la disrupción de la tecnología blockchain. Y las empresas de telecomunicaciones no son una excepción. La base de esta disrupción es la confianza, pero no aquella que se da entre las partes o la que tiene que ver con la seguridad, sino la que genera el diseño del propio sistema blockchain, que va a permitir a diferentes industrias interoperar entre sí de tal modo que surgirán nuevos modelos de negocio en el sector de las telecomunicaciones que hasta ahora no eran posibles ni viables. A primera vista podemos identificar cuatro aspectos del negocio de las telecomunicaciones que se verán afectados:

1. La gestión interna de las redes.
2. La gestión interna del negocio.
3. La provisión de los nuevos servicios de telecomunicaciones y la innovación que la blockchain puede añadir a éstos.
4. La bajada de las barreras de entrada que el sector de telecomunicaciones tiene de manera natural, lo que posibilitará una nueva oleada de competencia en el sector.

A continuación explicamos estos cuatro aspectos en detalle.

La gestión interna de las redes con blockchain

Las de telecomunicaciones son compañías con millones de clientes que atender, millones de elementos de red y dispositivos que gestionar —billones en un futuro cercano con el internet de las cosas (IoT)—, y miles de fuentes distintas de información de red que procesar y coordinar. Esto significa que cualquier automatismo que reduzca la complejidad de dicha gestión acabará por imponerse. Ahí precisamente es donde entra en juego la blockchain, que no es sino una tecnología de automatismos de gestión: de gestión de autenticidad —

pues se basa en hashes—, de gestión de duplicidades —dado que es un registro único, un ledger o libro mayor— y de gestión de seguridad —porque impide la falsificación y, por tanto, el fraude—. Por eso, utilizar una blockchain en el mundo de las telecomunicaciones es algo natural.

Sumemos a todo esto que se acerca una nueva generación móvil, la quinta (el 5G), que además de la promesa de elevadas velocidades de transmisión de información (del orden de gigabytes por segundo) proporcionará también una estructura de red flexible, distribuida y adaptable. Todo ello será posible gracias a la virtualización de las funciones de la red (Network Function Virtualization o NFV) y a la propia definición de redes mediante software (Software Defined Networks o SDN).

Esta tecnología 5G permitirá definir diferentes tipos de redes móviles sobre una misma infraestructura (lo que se llama «rebanadas de red» o *network slices*), de forma que se podrán satisfacer los requerimientos técnicos que los diferentes sectores industriales puedan demandar de las redes de telecomunicaciones. Por ejemplo, los servicios de coches autoconducidos, que requerirán de redes altamente fiables que reaccionen en milésimas de segundo, o los servicios de salud remota (e-Health), que exigirán, sobre todo, máximas garantías de privacidad y seguridad.

La 5G está pensada, entre otras cosas, para permitir que las redes gestionen billones de dispositivos autónomos en el internet de las cosas, dispositivos que se identificarán utilizando software y se autoprovisionarán en los sistemas de un operador. La blockchain podría ser esa tecnología de identificación que complemente —o incluso sustituya en algunos supuestos— a la conocida tarjeta SIM (en realidad al IMSI o International Mobile Subscriber Identity). De este modo resultaría sencillo comprobar previamente que un dispositivo que se quiere activar en una red por primera vez es quien dice ser antes de iniciar la carga de la identidad móvil en dicho dispositivo. Es más, la blockchain incluso podría permitir el uso de la red de un operador de manera discreta (puntual) por parte de dispositivos que sólo necesitan hacerlo una vez —dispositivos de «usar y tirar»—, lo que evitaría el malgasto de las identidades propiamente móviles (IMSIs, un recurso escaso).

Otra característica de la 5G es que posibilita que las redes actúen a partir de «estímulos externos», esto es, que terceros actores (otras industrias), mediante el uso de interfaces de programación de aplicaciones (API, por sus siglas en inglés), demanden a las redes que se configuren de manera concreta, bien solicitando más recursos, bien cambiando su topología. Así, la tecnología blockchain podría comportar mejoras en la autogestión de la red, porque permite confirmar la identidad de quien está pidiendo dichos cambios de manera inequívoca y cuasi inmediata. La flexibilidad y agilidad, desconocidas hasta la fecha, que todo esto comporta harán posible establecer modelos de negocio totalmente nuevos entre los operadores y las industrias que utilizan sus servicios, así como ofrecer servicios mayoristas que por su complejidad son hoy inviables.

Además, la blockchain trae un «regalo» añadido y de capital importancia: la invulnerabilidad a ataques exteriores debido a la seguridad de su diseño, lo que se conoce como *Security by Design*. Ello la hace perfecta para la gestión de una infraestructura crítica como es la de las telecomunicaciones. Es cierto que en estos aspectos de seguridad una blockchain privada es más débil que una blockchain pública, pero ya existen híbridos de blockchain que aúnan las ventajas de ambas; la seguridad ante ataques de fuerza (propia de la pública) y la flexibilidad de uso (de la privada). Este aspecto de la seguridad adquiere mayor relevancia aún si se considera el aspecto estratégico que las redes de telecomunicaciones tienen para los Estados en un entorno internacional como el actual, marcado por la amenaza de ciberataques.

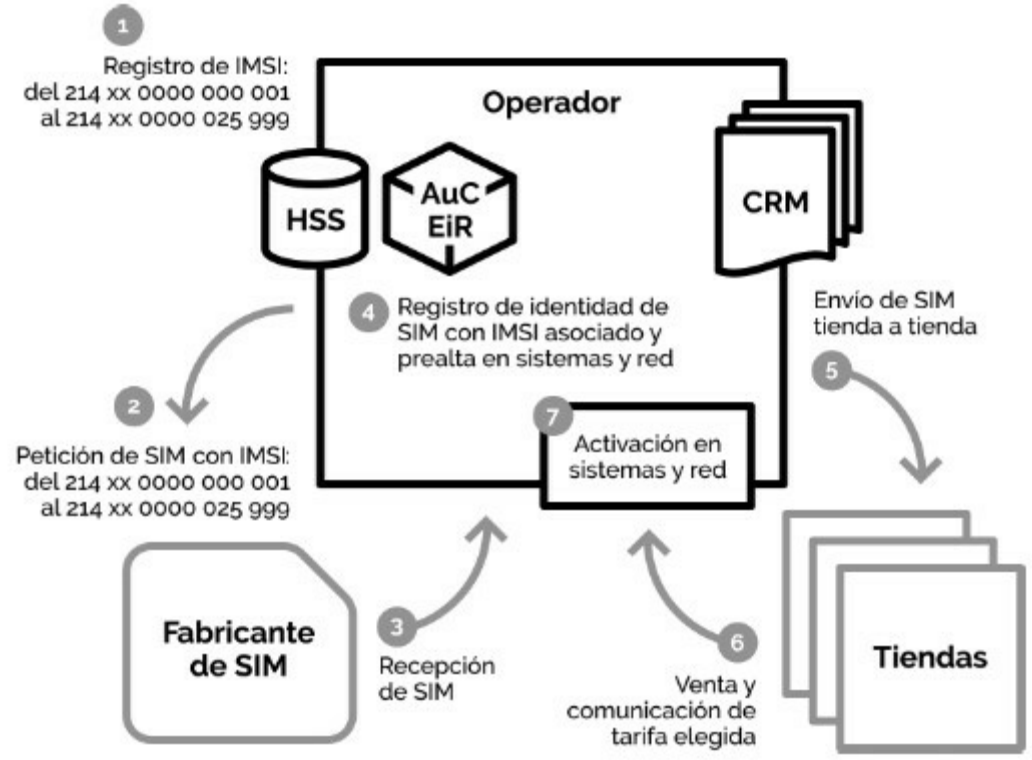
Gestión interna del negocio de un operador de telecomunicaciones

Si uno se detiene a pensar un poco en el sector de las telecomunicaciones, le será fácil ver que una operadora se dedica principalmente a llevar datos (datos IP, la voz y los SMS) de un origen a un destino. Pero si vamos un poco más allá, descubriremos que, especialmente los operadores móviles, son también grandes empresas de logística.

Tarjetas y móviles deben estar disponibles al público en prácticamente cualquier lugar de la geografía nacional a través de tiendas o puntos de distribución. Ahí son almacenados en estado latente (no activo) hasta su venta.

Materializada ésta, se activan en función de las preferencias del cliente y se le asigna la tarifa elegida. En este proceso, una operadora de telecomunicaciones difiere poco de quien se ocupa de enviar paquetes de un sitio a otro, de gestionar contenedores alrededor del mundo o de controlar la producción en función de las ventas en tiempo real.

Esquema del proceso de activación de una SIM.



Si tomamos como ejemplo las tarjetas SIM, un operador debe pedirlas a su proveedor, proporcionando la numeración IMSI asociada (y previamente asignada por la entidad reguladora del país donde opera el operador). Una vez fabricadas son enviadas a cada tienda o distribuidor y registradas en las bases de datos, tanto en la red móvil (en los HSS o Home Subscriber Server, en el AuC o Autentication Center y en el EIR o Equipment Identification Register) como en los sistemas de gestión de la propia SIM (averías, terminal asociado, etc.). Una vez vendidas y activadas, se incorporan a los sistemas de cliente (marketing, facturación, etc.) con sus datos personales.

Cada uno de dichos pasos lleva consigo un proceso de verificación y de seguridad que los hace muy lentos (incluso más que el control de paquetería tradicional) por la cantidad de comprobaciones requeridas. Aquí es donde la

blockchain podría automatizar prácticamente todo el proceso, de modo que los tiempos de retraso queden limitados a los puramente necesarios por el transporte físico.

Todo lo dicho te quedará claro a través de un ejemplo que seguramente conoces bien por propia experiencia: la portabilidad de los dispositivos y las SIM entre operadores. Si has hecho alguna sabrás que esa portabilidad no es inmediata, pues para que se dé es necesario cierta sincronización entre donante y receptor. Es decir, que la red receptora debe registrar al nuevo cliente después de que la red donante lo haya dado de baja en sus sistemas y en la base de datos centralizada (la ledger de la portabilidad). Sin duda, se trata de una medida razonable para que el móvil no se vuelva «loco» y se registre en dos redes diferentes a la vez, pero ello no quita que el proceso sea lento. En cambio, con la automatización que posibilita la blockchain, la portabilidad sería prácticamente inmediata.

Interoperabilidad entre sectores con blockchain

Todo lo explicado anteriormente sobre las ventajas que la blockchain traería a la gestión interna del negocio es extrapolable al lanzamiento de nuevos servicios, tanto por la mejora, simplificación y abaratamiento de los procesos propios de éstos como por la posibilidad de utilizar esta tecnología para hacer interoperar los sistemas de diferentes sectores. En lo que se refiere a la simplificación y mejora de los procesos internos, ya hemos mencionado la posibilidad de que las redes se utilicen una sola vez («usar y tirar») o que los operadores pongan a disposición de terceros nuevos servicios mayoristas. Aquí se abre la puerta a que otros sectores de la industria innoven en la manera que ofrecen sus servicios. Pero es que la blockchain, además, permitirá que un operador pueda utilizar los Smart Contracts en la comercialización, de forma que no sea necesario que un cliente tenga cuenta asociada al operador móvil para poder utilizar un servicio prepago. En este supuesto bastará con que tenga cuenta en cualquier entidad bancaria capaz de interoperar con el operador móvil. Esto aseguraría, por ejemplo, la devolución automática en nuestra cuenta del saldo si no lo hemos consumido en seis meses, o que podamos utilizar diferentes cuentas sin necesidad de avisar al operador para que cambie sus domiciliaciones.

La privacidad y seguridad de los datos personales

Esta interoperabilidad entre los servicios de diferentes industrias permitirá una nueva ola de innovación en la oferta. Hoy mismo, los usuarios de internet obtienen servicios gratuitos gracias a que permiten que las empresas comercien y utilicen sus datos personales, su identidad digital. Esta explotación, sin embargo, la llevan a cabo las empresas de internet, no los operadores. Esto significa que no se conoce quién puede tener nuestros datos ni qué uso se hace de ellos, por lo que no es de extrañar que la preocupación por la privacidad y seguridad de toda esta información aumente cada día.

Telefónica, por ejemplo, lleva años trabajando en una plataforma que permita devolver al usuario el control de sus datos, y en su caso, de los beneficios de su uso. En este campo, la blockchain puede jugar un papel diferencial, de forma similar a cómo se plantea el uso de esta tecnología en el terreno de la propiedad intelectual. Sirva como ejemplo la música: si alguien utiliza mis canciones (datos), automáticamente obtengo el beneficio (*revenue share*) de dicho uso a través de un Smart Contract.

La combinación de estas plataformas con la identidad digital del cliente —que empoderan al propio cliente con su control—, unido a la capacidad que la blockchain provee de interoperabilidad, podría elevar el concepto de portabilidad a un nivel que hoy se desconoce, haciendo posible que un usuario pueda mover de una aplicación a otra, y de forma sencilla, todos sus contenidos subidos a internet.

Reducción de las barreras de entrada en el sector de las telecomunicaciones con blockchain

Por otro lado, todas las oportunidades que la blockchain ofrece a los operadores también significan una amenaza. Toda disrupción de un negocio propicia ganadores y perdedores, de modo que algunas compañías se afianzarán como líderes en el sector, aparecerán otras más flexibles y que se adapten mejor a los «nuevos tiempos», y las habrá también que saldrán peor paradas e irán languideciendo lentamente, incapaces de adaptarse al cambio, hasta su total desaparición.

Las ventajas que ofrece la blockchain serán aprovechadas por las compañías más ágiles, lo que se traducirá en operadores de pequeño tamaño y poca plantilla (como los operadores móviles virtuales o OMV), capaces de gestionar mucho más eficazmente grandes cantidades de clientes (o clientes-cosas en IoT). De este modo se recrudecerá la competencia en el sector de las telecomunicaciones, lo que siempre acaba generando beneficios para la sociedad. Pero, además, disrupciones como las que representan Airbnb, Uber o Car2Go indican que los nuevos competidores no vendrán únicamente del propio sector, sino que probablemente lo hagan también de otros adyacentes y con propuestas rompedoras que añadirán otro punto de competitividad a las telecomunicaciones.

Queda claro, pues, que el uso de la tecnología blockchain está plenamente justificado en el mundo de las telecomunicaciones, tanto por las ventajas intrínsecas que comporta para el propio sector como por las posibilidades de interoperabilidad con otros que ofrece.

Más información sobre el impacto de la blockchain para las telecomunicaciones en <libroblockchain.com/telecomunicaciones/>.

Un nuevo modelo energético innovado a la vista

Ignacio Madrid Benito

La industria energética, de tanta importancia estratégica para el desarrollo del país, se encamina hacia una descentralización que cambiará por completo las reglas de juego del sector, pues traerá consigo el incremento del número de activos y la reubicación de los mismos. En la actualidad, la demanda energética de un país como España está cubierta por cerca de mil centrales más o menos grandes, ubicadas lejos de los grandes centros de consumo. En un futuro cercano serán sustituidas por decenas de miles de centrales, algunas tan grandes como las actuales y muchas otras medianas o pequeñas, situadas en distintos lugares, pero mucho más cerca del consumidor final. Tanto, que en algunos casos estarán incluso en la propia instalación de ese consumidor, por ejemplo, en el tejado de su casa o empresa. Gracias a la redistribución de estas nuevas pequeñas centrales de generación, la gestión del sistema eléctrico se podrá realizar de manera local, de modo que se aplique un ajuste eficiente y se puedan solucionar incidencias a pequeña escala, evitándose así ineficiencias a las que hasta hoy no se podía hacer frente.

La infraestructura[14] de las empresas distribuidoras tendrá que adaptarse a este nuevo modelo de gestión local de las redes, ya que el número de interlocutores se multiplicará por miles. Y no sólo eso, sino que se pasará de un modelo en el que la energía va en un solo sentido, desde las plantas de generación al lugar de consumo, a otro en red en el que la energía se mueve en cualquier sentido. Todo eso en un modelo donde las plantas de generación pueden estar ubicadas en cualquier punto de la red e inyectar electricidad en cualquier sentido, lo que afectará al modelo de gestión tradicional.

Con la entrada de pequeños «prosumidores» (consumidores que cuentan con su propia fuente de generación de energía) cambia también el modelo de gestión de los activos de distribución, ya que si antes las propias compañías distribuidoras eran las propietarias de los equipos de actuación, ahora éstos pueden ser de los propios consumidores. Esto no sólo comporta una

transformación en el modelo de inversión en infraestructura, sino que trae consigo importantes eficiencias al utilizar de manera inteligente todos los activos disponibles, propios y de terceros.

Si a todo lo anterior sumamos las posibilidades que supone el almacenamiento de energía a pequeña escala y la gestión activa del lado de la demanda (tener la capacidad no sólo de generar más, sino también de reducir el consumo en momentos de exceso de demanda de manera remota), las posibilidades de optimizar el sistema son infinitas.

Las tecnologías de la revolución energética descentralizada

El avance en las comunicaciones y en la capacidad de análisis de la información ha facilitado el debate sobre este nuevo modelo energético. La tecnología que será la base de este sistema eléctrico está ya disponible, pues tanto los contadores inteligentes[15] como las instalaciones solares fotovoltaicas conectadas a internet, las baterías de litio con módulos de gestión inteligente o los edificios con sistemas de control remoto permiten ya dotar al sistema eléctrico de importantes mejoras y flexibilidad. El gran reto de este nuevo concepto reside en la capacidad de gestión de los activos disponibles, las tipologías y los acuerdos establecidos entre las distintas partes.

La irrupción de la blockchain en el sector representa, sin duda, un impulso decisivo para la implantación de ese nuevo modelo de sistema eléctrico. Aunque los ejemplos de aplicación son muy básicos aún, compañías como Siemens[16] han apostado ya por proyectos de aplicación de la blockchain a la generación distribuida. El resultado ha sido la compañía LO3 que, junto con ConsenSys, ha desarrollado en Brooklyn (Estados Unidos) un programa piloto sobre las ventajas de un sistema descentralizado basado en la blockchain.

La generación distribuida y los autoconsumidores

Gracias a la evolución de las tecnologías de generación a pequeña escala (solar, eólica, biomasa…), los consumidores pueden generar su propia electricidad o parte de ella mientras siguen conectados al sistema existente. De este modo el consumidor (o autoconsumidor) consigue solventar esos momentos en los que

la generación propia no es suficiente para cubrir su demanda y, por otro lado, tiene la posibilidad de vender los excedentes[17] al mercado o a un consumidor en particular, según se establezca en un contrato bilateral. Esta nueva realidad abre el sistema a un gran número de nuevos interlocutores, no profesionalizados y de tamaño muy reducido, que podrían incidir tanto en la operación física del sistema como en la liquidación diaria de la energía.

Iniciativas como Powerpeers,[18] secundada en los Países Bajos por la eléctrica Vattenfall, hacen que sea ya posible la compraventa de energía punto a punto, y ello gracias a experimentos con la blockchain. Otro proyecto interesante, Grid Singularity, se orienta a asegurar las transacciones entre pequeños generadores de energía solar y consumidores en países en vías de desarrollo.

El almacenamiento en baterías

La llegada de las nuevas baterías pone en jaque las bases del sistema eléctrico al introducir nuevas opciones para la gestión física de la electricidad. En un sistema distribuido es el complemento perfecto para los autoconsumidores, ya que les permite almacenar el excedente de energía en la batería y utilizarla cuando no haya sol o viento, o venderla al mercado en el momento en que el precio sea más elevado. De este modo, cada batería será una nueva variable en el sistema y un nuevo agente con voz en el mercado eléctrico. Compañías como la australiana Power Ledger ya están experimentando con proyectos[19] que van en esa vía.

La flexibilidad y la gestión de la demanda

La irrupción del internet de las cosas ha acelerado el mercado de la gestión inteligente de los equipos de consumo, desde edificios con complejos sistemas de control y capaces de activar y desactivar cualquier equipo que consuma energía, hasta sencillos sistemas de calefacción individual en las casas. Gracias a estas tecnologías, el consumidor puede poner sus equipos consumidores al servicio del sistema, de forma que éste pueda variar su funcionamiento y, por tanto, su consumo, previo acuerdo de los niveles de confort (por ejemplo, la temperatura de climatización entre 2°C y 4°C) y a cambio de importantes beneficios económicos.

Con la entrada de esta tipología de acuerdo y estas nuevas tecnologías, el sistema eléctrico se expande mucho más allá de la mera generación y distribución tradicional, y sube un punto más su nivel de complejidad. En Alemania, por ejemplo, ya se está trabajando en esta línea con proyectos de la blockchain como NEW 4.0,[20] que pretende ser el primer Smart Market para flexibilidad.

Los agregadores: «Virtual Power Plants»

Para los agentes pequeños resulta poco operativo actuar individualmente en el mercado, e igualmente su posible aportación es de poco interés para el sistema. Para solucionar eso se ha puesto en marcha el VPP (Virtual Power Plant), una iniciativa que trata de agrupar a los pequeños generadores, acumuladores o, sencillamente, edificios conectados a fin de operar de manera única en el mercado, entrando de este modo en competencia con las grandes centrales de generación. Los responsables de estas VPP son los encargados de la gestión interna de los compromisos adquiridos con el sistema y para ello están conectados con todos los activos en remoto. Estos entes pueden calcular en tiempo real su capacidad agregada para ofrecerla al mercado, decidir cómo actuar de manera óptima y, hecho eso, liquidar los importes con cada una de las pequeñas partes involucradas. Esta agrupación no es física, sino virtual, ya que la energía ni se inyecta ni se agrega en un punto.

Movilidad eléctrica

La energía almacenable en un coche eléctrico actual es equivalente al consumo de dos días de un hogar medio. Siendo esto así, la electricidad disponible en el parque móvil —en un escenario de alta penetración de la movilidad eléctrica— sería de máximo interés para la optimización del sistema eléctrico. Pero la posibilidad de dejar un coche enchufado y que la propia red eléctrica pueda disponer tanto de la energía de las baterías de los coches como del almacenamiento disponible para gestionar el balance de la red, hace compleja la gestión. Es por esto que RWE, una de las mayores eléctricas de Europa, ha lanzado un proyecto[21] junto con Slock.it para gestionar la carga de los coches eléctricos mediante los Smart Contracts sobre Ethereum.

La electrificación y el futuro

En un escenario de generación renovable como el que se dará en los próximos años, la electrificación del mayor número de equipos consumidores de energía resulta de gran interés desde el punto de vista medioambiental (y seguramente económico). Los analistas estiman que en 2030 la demanda de energía eléctrica aumentará en un 30% debido fundamentalmente a dos motivos: por un lado, la electrificación del transporte gracias al impulso de la movilidad eléctrica como alternativa real a los combustibles fósiles; por otro, la electrificación de los sistemas de calefacción, que supondrán un aumento de casi un 8% de la demanda eléctrica. Por tanto, cada vez serán más los activos conectados al sistema eléctrico y cada vez más importante su gestión. El facilitador de esta transición no será otro que la blockchain.

Más información sobre el impacto de la blockchain en el sector eléctrico en <libroblockchain.com/energia/>.

La industria 4.0 y la blockchain

Óscar Lage Serrano

Nos encontramos en los prolegómenos de lo que los expertos denominan la «cuarta revolución industrial». La digitalización y coordinación cooperativa de las unidades productivas van a suponer un nuevo hito en el desarrollo industrial, como en su día lo supusieron los tres anteriores cambios disruptivos: la máquina de vapor y la mecanización, el desarrollo de la electricidad y la producción masiva, y la automatización avanzada del proceso de fabricación gracias a la electrónica y a las tecnologías de la información.

En la actualidad, la demanda es cada vez más sofisticada y requiere productos más inteligentes y personalizados. Esto supone un nuevo paradigma tanto para las empresas productoras como para la propia industria manufacturera. Las primeras deben dar el salto a la creación de soluciones personalizadas —en las que el hardware supone únicamente una parte del servicio— y dirigirse cada vez más hacia modelos de negocio basados en el servicio y el pago por uso. Al mismo tiempo, la industria manufacturera deberá ser capaz de adaptar el actual sistema de fabricación, concebido en grandes lotes de productos, hacia otro en el que impere la personalización. El objetivo de la cuarta revolución industrial, de hecho, viene definido por nuevas fábricas inteligentes, capaces de producir miles de configuraciones diferentes de un producto y de fabricar pequeños lotes o lotes unitarios a precios muy reducidos que puedan competir con los precios actuales de la producción masiva. El concepto de las grandes plantas de fabricación masiva no tendrá cabida en este nuevo escenario.

La digitalización es la base de esta revolución industrial, lo que dará como resultado la denominada «industria inteligente», sustentada en tecnologías facilitadoras como son el internet de las cosas (IoT), las comunicaciones Machine to Machine (M2M), las plataformas en la nube, los robots inteligentes, la impresión 3D, etc. Los datos, además, tendrán un mayor valor en el negocio, de modo que no serán ya un mero resultado del proceso de fabricación (necesario en todo caso para soportar procesos de planificación y optimización), sino la base del producto o servicio, o incluso el propio producto en sí mismo.

Por esta razón se están lanzando diferentes iniciativas denominadas Industrial Data Platform dirigidas a gestionar y compartir datos de los procesos de fabricación, así como a crear servicios de valor añadido sobre los mismos, como puede ser el caso del mantenimiento predictivo. Algunas de las plataformas emergentes en este ámbito son Industrial Data Space,[22] Mindsphere de Siemens o Digital Manufacturing Commons (DMC), liderada por GE y UI Labs.

Como toda innovación disruptiva, estos cambios en el modelo de negocio traen consigo nuevos retos tecnológicos. A continuación revisamos aquellos a los que la blockchain puede dar respuesta.

Autenticación e integridad de datos en dispositivos industriales

El internet de las cosas es una tecnología tan relevante en esta nueva revolución industrial que incluso ha recibido una denominación determinada: Industrial Internet of Things (IIoT). Las necesidades específicas del sector industrial justifican tal nombre ya que, a diferencia del mercado de consumo, los dispositivos en este ámbito deben formar parte de ecosistemas amplios, escalables e integrables en los diferentes sistemas empresariales. La gestión descentralizada de la identidad de dichos dispositivos cobra así una vital importancia. Aunque su autenticación y sus comunicaciones representan un reto en la industria IoT en general (véase OWASP IoT Top 10 vulnerabilities),[23] dentro de un contexto industrial adquieren mucha más relevancia, ya que se trata de sistemas ciberfísicos que pueden incluso poner en riesgo vidas humanas.

La blockchain se postula como una de las posibles soluciones al reto de la identidad de los dispositivos IoT y en particular de IIoT, pues a diferencia de las soluciones centralizadas tradicionales ofrece una gestión de identidad descentralizada. De hecho, la descentralización de la identidad es una de las fortalezas de esta tecnología. En blockchain se puede verificar la identidad de dichos dispositivos sin depender de una autoridad de certificación centralizada (Certification Authority, CA) difícil de gestionar y que puede convertirse en un punto único de fallo del sistema. Además, en la actualidad las soluciones industriales requieren del despliegue de una CA por cada fabricante industrial o

del uso de una CA de fabricante que la industria no gestiona directamente, lo que provoca no sólo una gran dependencia de sus proveedores, sino también incertidumbre y falta de control.

La descentralización de la blockchain, por tanto, puede suponer una ventaja importante en el paradigma IIoT, pues gracias a las características intrínsecas de esta tecnología será posible registrar la actividad de cada sensor/actuador en la red industrial y garantizar así la integridad de los datos generados por la IIoT, sin miedo a la manipulación de registros y sus consecuencias. Cabe señalar también que el registro inalterable de los valores de la IIoT mediante tecnologías blockchain puede ser muy útil para el análisis forense de cualquier incidente que afecte a una infraestructura crítica, como el sector energético o las industrias químicas. En los últimos años han surgido diferentes normativas para la identificación y protección de estas infraestructuras críticas que así lo aconsejan.

Transacciones M2M en la blockchain

La fábrica inteligente del futuro estará compuesta por dispositivos IIoT y/o por módulos de fabricación conectados entre sí y que funcionarán de forma autogestionada o autosuficiente. De esta forma, y mediante el uso de tecnologías como la blockchain, surgirá una nueva economía en la que los propios dispositivos, mediante comunicaciones M2M, serán capaces de llegar a acuerdos de suministro de materias primas, piezas, mantenimiento, energía y delegación/ coordinación de la producción, e incluso también logísticos, que quedarán reflejados en los Smart Contracts y cuyo pago se ejecutará automáticamente cuando se cumplan las condiciones establecidas en el contrato. La intermediación de terceros en las transacciones, incluso la interacción humana, se verá así disminuida en gran medida. En este sentido, ya se están realizando los primeros micropagos piloto basados en la blockchain, por ejemplo, entre coches y puntos de recarga o autopistas, sensores que venden sus datos, etcétera.

Los marketplaces industriales y la blockchain

Automatizar y agilizar ciertos procesos actuales es la condición básica para que la fabricación inteligente pueda llegar a producir lotes unitarios en el mismo rango de precios que los ofertados por la fabricación de grandes volúmenes de

la actualidad. Entre esos procesos se hallan la recepción y confección de ofertas, las órdenes de fabricación, la gestión logística o los pagos de cada uno de esos minúsculos lotes de fabricación. De no ser así, los costes indirectos que se deberán amortizar por cada lote unitario podrían superar el coste de fabricación del propio producto, como ocurre en la actualidad.

Se hace necesario, por tanto, automatizar estas transacciones y para ello no sirven los actuales portales web de proveedores, en los que los clientes realizan pedidos y luego son atendidos de forma manual, ni tampoco los intermediarios que ofrecen servicios, tan habituales hoy en la nueva economía digital. Ejemplos recurrentes de esto último son empresas como Airbnb o Booking.com que, por su papel intermediador, se quedan con un margen de los bienes y servicios ofertados por terceros.

Según los expertos en la denominada industria 4.0,[24] la solución pasa por la desintermediación del proceso productivo, de forma que las empresas puedan recibir las peticiones desde un portal descentralizado y fabricar lotes pequeños o incluso unitarios. El acercamiento físico entre el ente productivo y el lugar de destino final del producto se ve de este modo propiciado, lo que repercute también en la reducción de costes logísticos y, a su vez, facilita que la fabricación pueda ser realizada por pequeñas pymes locales, que cooperan de forma coordinada para ofrecer este servicio de fabricación integral.

Esa plataforma descentralizada es posible gracias a la blockchain. Un Smart Contract cerrará automáticamente el acuerdo con la mejor oferta sin necesidad de intervención de ninguna de las partes. Un ejemplo de ello en otro contexto es OpenBazaar, una alternativa distribuida y gratuita que pretende competir con soluciones intermediadas como eBay.

Más información sobre el impacto de la blockchain en la industria 4.0 en <libroblockchain.com/industria40/>.

Farma y salud dan un paso al frente

Dioni Nespral

Vivimos en un mundo en el que consumimos ingentes cantidades de información y en el que demandamos cada vez más conocimiento preciso de aquello que nos preocupa, nos interesa o nos ilusiona. Y esta tendencia irá a más, pues la próxima década será la de la gestión, inteligencia, transparencia y personalización de la información más relevante para cada uno de nosotros, incluida, por supuesto, la referida a la salud. Administraciones sanitarias e industrias farmacéuticas son conscientes de los grandes retos que esto supone (entre otros, el incremento anual sostenible del gasto sanitario en las economías más avanzadas, la búsqueda de una mayor eficiencia y la mejora constante del servicio al paciente) y del importante papel que la blockchain puede jugar en su solución. En este escenario global están llamados a participar todos los actores del sector: las grandes industrias farmacéuticas, los distribuidores, los centros hospitalarios y los profesionales médicos y farmacéuticos.[25] Porque el éxito no llegará de la mano de soluciones aisladas, sino que requiere de una visión global y de una gestión coordinada y moderna.

La tecnología ha de jugar un papel relevante en esta transformación del sector de la salud. Entre los proyectos tecnológicos emprendidos en este ámbito destaca CRAVIB (Crowdsourcing, Robotics, Artificial Intelligence, Virtual Reality and Blockchain), que se plantea un doble reto: por un lado, proporcionar una solución que haga evolucionar la situación actual hacia modelos más modernos, avanzados y flexibles que posibiliten la nueva estructura en el sector; por otro, ser un potente vehículo de desarrollo social, económico y ambiental para la sociedad en general, y para el sector y sus agentes en particular.

Ante este escenario actual y futuro, la blockchain se presenta como un elemento clave para garantizar la seguridad, fiabilidad y transparencia de la información. Hoy ya son muchas las empresas innovadoras que están posicionándose para ser protagonistas de la nueva era posdigital.

Farma y blockchain, nacidas para trabajar juntas

En el sector sanitario hay un interés evidente por resolver las lagunas que resultan del desfase de velocidad y adaptación con el entorno social en el que vivimos. Hasta ahora, ha podido sobrevivir ajustando o poniendo parches temporales frente a las crecientes demandas empresariales y sociales, pero frente a una sociedad instantánea, dinámica y cada vez más transparente e informada como la de hoy, esto no es ya suficiente. Se hace necesario resolver problemas como la relación directa entre los actores involucrados, la eficacia en las operaciones logísticas de amplia distribución, la detección de fraudes en los medicamentos y la necesidad de disponer de información incorruptible, transparente y actualizada.

Por otro lado, el paciente quiere información precisa sobre su historial médico, sus tratamientos, la utilización de sus datos y la propiedad de dicha información. El avance de una información más distribuida y compartida con los agentes del sector debe tener en cuenta las necesidades, la individualidad y las demandas de cada paciente. El resultado deseado es conocido, pero la ecuación debe estar bien formulada. Y la blockchain es parte de esa ecuación.

Blockchain, gestión farmacéutica y distribución no fraudulenta de medicamentos

La tecnología blockchain permite estar mejor preparados frente a las falsificaciones o fraudes, autenticando el origen y distribución de los fármacos, eliminando la posibilidad de fraude en la cadena y luchando frente a los fabricantes ilegales de medicamentos.[26]

Las compañías pueden desarrollar blockchains privadas en las que involucrar a los agentes productores, distribuidores, vendedores, etc., y lograr integrarlos en todos los nodos de la cadena. Cada vez que un medicamento es fabricado, se genera un hash que proporciona toda la información relativa a su fabricación y componentes. Y cada vez que un agente interacciona con ese medicamento, se vuelve a generar otro hash vinculado al anterior con más información, lo cual podría permitir una trazabilidad total, fiable y transparente. Entre los proyectos que trabajan ya sobre esta problemática figura una compañía como Blockverify,[27] que desarrolla servicios sobre transparencia en las cadenas de suministro de diversas industrias, farmacéutica incluida.

Aunque ya existen compañías privadas que están desarrollando aplicaciones blockchain propias, es interesante destacar iniciativas como iSolve[28] o BlockRx,[29] que tratan de optimizar la operativa diaria en campos como la protección de la información confidencial en el I+D de los nuevos medicamentos o la eficaz distribución de los mismos a lo largo de toda la cadena de suministros. Asimismo, un correcto uso de la tecnología blockchain permitiría a los usuarios finales tener un control sobre el origen de los medicamentos a través de la implementación de los contratos inteligentes o Smart Contracts que abrirían la puerta a modelos de relación y comercialización no contemplados en la actualidad.

La blockchain, nueva relación de los agentes en el ámbito de la salud y los pacientes

En una sociedad tan abierta como la nuestra se hace necesario reinventar la relación entre el sector sanitario y los pacientes, especialmente en un tema tan controvertido como la confidencialidad y la información puesta a disposición de los investigadores. La blockchain puede ser también una herramienta para lograr nuevos modelos en este ámbito, como lo demuestra Blockchain Health Co.,[30] una iniciativa que busca establecer una relación directa entre pacientes e investigadores. Gracias a la tecnología blockchain es posible gestionar adecuadamente la información sensible y el acceso a los datos de los pacientes.

Otro ejemplo es The BlockRx Project, que está explorando la posibilidad de recopilar datos de los pacientes tanto para reducir costes como para acelerar los resultados de las investigaciones a través de la expansión de un conocimiento conectado y distribuido. Todo ello con el objetivo de lograr un modelo más eficiente, cercano y fidedigno que, al mismo tiempo, asegure la confidencialidad de los actores involucrados y evite pérdidas, en algunos casos millonarias, a las compañías que gestionan datos tan sensibles.

El sector público es uno de los más interesados en potenciar el uso de la blockchain. Un ejemplo de ello es Guardtime[31]que, impulsado por el Gobierno de Estonia, busca garantizar la seguridad y, a la vez, la constante actualización de los historiales médicos de sus ciudadanos mediante una base de datos descentralizada. Igualmente, existen soluciones para que los propios pacientes puedan acceder a su información personal y gestionarla. En esta línea, la

compañía HealthNautica utiliza los servicios proporcionados por el protocolo de Factom para una mejor gestión y verificación de los tratamientos de sus pacientes. Otras iniciativas relevantes —como PokitdoK—[32] conectan entre sí a pacientes y médicos con el fin de ofertar y contratar servicios directamente.

Todos estos ejemplos dan cuenta de una nueva forma de entender las relaciones entre los agentes del sector y los pacientes, que ha de traducirse en un entorno más fiable, transparente y saludable.

Más información sobre el impacto de la blockchain para el sector farmacéutico y sanitario en <libroblockchain.com/salud-farmaceuticas/>.

Pymes: eficientes y optimizadas

Roberto Díaz Bartolomé

Hace mucho tiempo ya que la inmensa mayoría de autónomos y pequeñas empresas utilizan herramientas digitales para gestionar sus negocios, como pueden ser las distintas soluciones de facturación y contabilidad en la nube. La tecnología blockchain que, en esencia, es un libro de contabilidad que registra transacciones digitales, ¿qué valor podría aportar en la gestión y a nivel operativo para autónomos y pymes?

El conocimiento del estado de las cuentas actualizado en tiempo real desde un smartphone, la contabilización automática de gastos y facturas recurrentes o la conciliación bancaria con un solo clic son ventajas evidentes y el paso previo a la automatización integral de todos los procesos que conforman la gestión de un negocio. De llevarse a cabo, esa automatización podría convertirse en una herramienta de inteligencia de negocio «a escala» que facilite la toma de decisiones en tiempo real.

La digitalización de la gestión de todo negocio, especialmente de los más pequeños, está aún dando sus primeros pasos, principalmente a causa de una lupa regulatoria dirigida a desincentivar el fraude, pero que actúa como barrera. Y es que en el sistema contable actual existen mecanismos de control mutuo que provocan mucha fricción a nivel operativo en el día a día de todo negocio, en especial, el trabajo doble que sistemáticamente llevan a cabo empresas e instituciones, además de toda la gestión documental y controles periódicos recurrentes. La mayor parte de estos procedimientos son manuales, requieren mucho tiempo y están lejos aún de automatizarse.

La blockchain, como el «libro distribuido», abierto y eficiente que es, tiene un potencial disruptor enorme en todo lo que se refiere a la contabilidad: permite desde simplificar requerimientos regulatorios hasta evolucionar el sistema de doble entrada que se usa en todo el mundo desde la época del Renacimiento.

El sistema de doble entrada en la blockchain

La contabilidad existe desde que el hombre hizo el primer trueque. Al fin y al cabo, es una manera de solventar los límites de la memoria humana y dejar constancia de que una transacción se ha llevado a cabo. En un primer momento se usó el sistema de entrada única. Esto era como una lista de tareas en la que se iban añadiendo las transacciones indicando su naturaleza y la cuantía del movimiento. El sistema funcionó hasta que el crecimiento del comercio y la creación de un tejido empresarial cada vez más complejo lo dejó desfasado.

Hacía falta otro método, y éste surgió en la Italia de finales del siglo XV y principios del XVI, la Italia del Renacimiento. Fue entonces cuando una familia de banqueros florentinos, los Médici, popularizó un sistema más robusto y fiable, el de doble entrada, que rápidamente se empezó a usar en negocios de todo el mundo. En él, cada transacción implica una contrapartida, de tal manera que siempre se verán afectadas como mínimo dos cuentas en los registros de una empresa: una con el débito y otra con el crédito. Es decir, un origen y un destino, de forma que toda aquella persona o entidad que vaya a auditar las cuentas del negocio pueda identificar rápidamente aquello que no cuadre y saber por qué.

¿Qué valor puede aportar la blockchain en la contabilidad de las pymes?

El sistema de doble entrada resolvía el problema que tenían los contables para saber si podían confiar en sus propios libros. Sin embargo, la intermediación de una tercera parte, los auditores, sigue siendo hoy necesaria para asegurar la integridad y fiabilidad de la información financiera. Y esto es un proceso enormemente costoso y lento que afecta a negocios de todo el mundo y que en algunas ocasiones tampoco ha resultado fiable.

La blockchain puede revolucionar la forma en que se llevan las cuentas de todo negocio: con ella ya no será necesario tener que mantener registros documentales de todas las operaciones realizadas, puesto que éstas quedarán registradas en una base de datos única y compartida por las partes necesarias, y ello en el mismo momento en que se efectúen. El resultado es un sistema encriptado, incorruptible y duradero.

Ya que todas las entradas estarán distribuidas y criptográficamente selladas, falsificarlas o destruirlas para cometer o encubrir fraudes sería mucho más complicado. Los beneficios que esto comporta para cualquier empresa son enormes, dado que la estandarización de los procesos contables a este nivel permitiría a usuarios externos verificar enormes porciones de información financiera de forma automática. El coste en tiempo y dinero se reduciría drásticamente, y ello tanto para las instituciones como para los auditores y asesores, que podrían dedicarse a ofrecer un servicio de mayor valor añadido.

Una blockchain como tercer libro de las pymes y empresas

Aunque el sistema de doble entrada ha permanecido en esencia intacto hasta el momento, Bitcoin nos ha enseñado que el futuro de la contabilidad puede pasar por el uso de un tercer libro, lo que da lugar a un sistema de triple entrada mucho más poderoso y útil que el usado hasta el momento.

Veremos cómo funciona mediante un ejemplo: imaginemos que la empresa A compra 100 € de algo que vende la empresa B. Hoy por hoy, esto implicaría que:

1. La empresa A contabilizará la transacción registrando la salida de efectivo (por ejemplo) y la entrada de un activo.
2. La empresa B contabilizará la transacción registrando la salida de un activo y la entrada de otro (dinero en efectivo, en este caso). Sin embargo, con un sistema de triple entrada añadiríamos otro paso:
3. La transacción se registraría al mismo tiempo, con la información pertinente, en una blockchain que la sellaría criptográficamente haciéndola inmodificable.

De esta forma, la transacción estaría registrada en los libros de cada entidad que participe de ella y, al mismo tiempo, en un libro genérico y disponible para ser consultado por terceras partes interesadas y a las que se les pudiera permitir el acceso, como podrían ser Hacienda, auditores, jueces, etcétera.

Integración a nivel institucional gracias a la blockchain

Uno de los mayores beneficios, si no el que más, que traerá la blockchain en este sentido será la integración total de las agencias tributarias en la contabilidad de las empresas. Al trabajar sobre una misma blockchain, se podrían elaborar estados contables y los distintos modelos de impuestos a presentar según la actividad de la empresa, y todo ello en tiempo real, sin necesidad de mantener los actuales procedimientos periódicos obligatorios requeridos por Hacienda. Resulta evidente el drástico ahorro en tiempo y dinero tanto para el propietario del negocio como para la administración que esto supondría.

Al mismo tiempo, esto ayudaría a la creación de una base de datos «viva», actualizada de forma orgánica y en tiempo real, tanto a nivel nacional como europeo, que permitiría pulsar en cualquier momento el estado de la economía a cualquier nivel y respecto de cualquier parámetro. De esta forma también podría atajarse el problema del fraude y la economía sumergida al asegurar una trazabilidad total de todas las operaciones llevadas a cabo por la empresa, además de un ahorro notable en multas derivadas del incumplimiento de los plazos requeridos en los procedimientos correspondientes.

En definitiva, la blockchain puede trascender la principal función que desempeñan los procesos contables para el pequeño empresario, en esencia la de cumplir con Hacienda. Y no sólo eso: puede también convertirse en una herramienta idónea para conocer el pulso del negocio de forma actualizada y, en función de la situación, favorecer la toma de mejores decisiones empresariales. En otras palabras, las pymes tendrían a su disposición un beneficio hasta ahora reservado a grandes empresas con enormes presupuestos dedicados a la inteligencia de negocio.

Más información sobre el impacto de la blockchain en pymes en <libroblockchain.com/pymes/>.

Juego online con la blockchain

Stefan Hamann

Desde sus inicios, la tecnología blockchain mantiene un estrecho vínculo con el sector del juego online. De hecho, y más allá de las transferencias de valor, la compraventa de tokens y la venta de productos en la deep web, los primeros casos de uso de Bitcoin se dieron en plataformas de juego como SatoshiDice. La transparencia y fácil auditabilidad propias de la blockchain podrían beneficiar a empresas y usuarios de este sector. ¿Cómo? Elevando a un nuevo nivel tecnológico cuestiones tan relevantes como el registro inmutable de las operaciones, el análisis de patrones de juego, la prevención del fraude o la creación de nuevos incentivos para los jugadores. El uso de los contratos inteligentes promete, además, un nuevo escenario en el que la resolución y ejecución de las apuestas se automatice de forma fiable, a prueba de cualquier manipulación.

Confianza en el juego online con la blockchain

En el año 2015, el volumen de negocio de las empresas de juego online alcanzó los 35.000 millones de euros.[33] Aunque este sector busca constantemente mejorar sus operaciones en un entorno competitivo de alto nivel, su apuesta por la tecnología blockchain es todavía cauta. Más que como una oportunidad, los operadores de juego online parecen haber percibido la blockchain como una amenaza para su negocio. Y eso que se trata de una tecnología que permite resolver los tres principales desafíos del juego online: la transparencia, la auditabilidad y la confianza, lo que podría traducirse en un nuevo y fuerte impulso del sector.

En ocasiones, las apuestas pueden ser una vía para el blanqueo de capitales (imaginemos el caso de alguien que compra un billete de lotería premiado para reclamar el premio en su nombre) y también para obtener rendimientos a partir de la posesión de información privilegiada, como por ejemplo el resultado de un evento concreto antes de que éste se produzca. Pues bien, todo esto se podría evitar gracias a la blockchain y las facilidades que ofrece para la identificación de los clientes (siguiendo los procedimientos habituales del Know-

YourCustomer, KYC) y para auditar las operaciones. De este modo, y acorde con la normativa contra el lavado de dinero (Anti-Money-Laundering, AML), resultaría imposible comprar un billete premiado a otra persona sin dejar rastro. Esta verificación de las identidades de los usuarios permitiría a éstos registrar[34] de manera segura información sensible como vídeos, fotos o grabaciones de audio como forma de identificación, información que a su vez podría ser usada por los operadores de juego para protegerse de reclamaciones injustificadas o reembolsos no autorizados, reduciendo así su responsabilidad legal.

Equidad y transparencia en el juego online con la blockchain

En el mundo de las apuestas, el usuario suele desconocer cuál es la lógica que opera tras las máquinas de juego. La blockchain, a partir de la base matemática que la sustenta, puede también solucionar este problema al mostrar a cualquier usuario que lo desee cuál es la probabilidad y aleatoriedad de las apuestas. De este modo, las reglas del juego se hacen más claras, lo que redunda en una mayor confianza y seguridad de los usuarios.

En la actualidad, la confianza del usuario en el proveedor es en buena parte subjetiva, pues depende de la reputación que este último tenga, lo que da pie a riesgos. Se trata, sin duda, de un campo susceptible de mejora, y también ahí puede tener un papel decisivo la tecnología blockchain. Si las apuestas o jugadas quedasen registradas en una base de datos descentralizada e inmutable, la integridad del juego quedaría garantizada, lo que a su vez asentaría la confianza de los jugadores, quienes probarían e interactuarían con las webs online de una manera más objetiva para medir su nivel de equidad y, por tanto, su atractivo.

La web de apuestas-bitcoin SatoshiDice[35] ha sido uno de los primeros casos en los que se ha hecho realidad este compromiso con las transparencia e integridad. Para ello se ha fijado una serie de opciones disponibles para apostar, con un componente aleatorio variable pero conocido para el jugador, y una recompensa automatizada, acorde a lo fácil o difícil que sea ganar la partida. SatoshiDice hace uso de la blockchain de Bitcoin: la combinación del hash cifrado del servidor de juegos, el hash del navegador del usuario y un nonce (conceptos estos que aparecen explicados con detalle en el capítulo dedicado a criptografía) genera un número o resultado aleatorio en un juego concreto.

Esta transparencia operativa aportada por la blockchain ha sido ya reconocida por organismos reguladores del juego como la Alderney Gambling Control Commission. Su director ejecutivo, André Wilsenach, defiende que la información «compartida, digitalizada y descentralizada» en un sistema de registro basado en la blockchain proporcionaría a los reguladores un acceso significativamente mejor a los datos requeridos.[36]

Segmentos del juego en los que la blockchain tiene mucho que decir

Los mercados de predicciones, las loterías o el póker son algunos de los segmentos del juego online que pueden verse más afectados por la tecnología blockchain.

Mercados de predicción y la blockchain

Los mercados de predicción son plataformas descentralizadas de intercambio comercial que recompensan a los usuarios por predecir eventos correctamente. Lo relevante de este tipo de mercados radica en la posibilidad de hacer uso de inteligencia colectiva para descontar la probabilidad de que se produzca un suceso. El protocolo Augur,[37] basado en Ethereum, es una plataforma para desarrollar mercados descentralizados peer-to-peer, que debido a su mayor simplicidad y eficiencia mediante el uso de su propio token (llamado REPutation) puede ofrecer unas condiciones más competitivas para los operadores tradicionales del sector.

Este uso de tokens, unido al férreo control de la identidad de los usuarios, permite eliminar los costes asociados al sistema bancario. Además, y acorde con la Directiva de Servicios de Pago aprobada en 2013 por la Comisión Europea (la Payment Service Providers, PSD2), prescinde de las tarjetas de crédito, algo que repercute positivamente en los costes transaccionales del cliente.

Mercado de loterías y la blockchain

Otro ámbito prometedor para la implementación de esta tecnología es la lotería. Uno de los casos de mayor interés aquí es el de Quanta,[38] una lotería blockchain que a la venta directa de billetes a cualquier persona suma una solución de marca blanca para que empresas o instituciones (como podría ser Loterías del

Estado) implementen la solución para uso propio. Quanta hace uso de contratos inteligentes sobre la red Ethereum para automatizar los diferentes procesos de la lotería, como la generación de números aleatorios, la emisión y almacenamiento de los billetes, la selección de los ganadores y el pago de los premios. Estos contratos inteligentes constituyen la columna vertebral de la lógica de la lotería: el desarrollador de la plataforma indica que Quanta promete «destinar» a premios hasta un 85 % de la venta de billetes, un porcentaje que supera notablemente el de las loterías tradicionales que, en el mejor de los casos, sólo distribuyen el 45% de los ingresos en forma de premios.

El póker y la blockchain

Uno de los juegos que más proyección ha tenido en internet ha sido el póker. Creada por la compañía especializada en el lanzamiento de soluciones tecnológicas de base blockchain, ConsenSys, Virtue Poker[39] utiliza la blockchain de Ethereum para retener los fondos mediante escrow hasta que termina el juego. Su protocolo permite a los usuarios jugar de manera colectiva e independiente, sin la necesidad de un tercero que supervise o arbitre el desarrollo de las partidas. La aplicación, sin embargo, no se ejecuta en la propia blockchain, ya que cada jugador utiliza una clave privada propia para garantizar que no haya manipulación en el juego de cartas. En cambio, los contratos inteligentes sí se generan y almacenan en la blockchain de Ethereum.

Estos contratos inteligentes se usan para garantizar los *buy-ins* (la cantidad de dinero exigida antes de que un jugador pueda incorporarse a la mesa de juego) de los torneos y, posteriormente, distribuir los pagos en función de los resultados. Por ejemplo, si tres personas quieren jugar en un torneo y apostar 20 ethers cada uno, se definen primero las normas del reparto del dinero (por ejemplo 40 ether para el primer clasificado y 20 ether para el segundo). Después, cada uno de estos jugadores envía 20 ether a un contrato inteligente en la blockchain de Ethereum desde sus carteras digitales. El resultado de la partida se plasma en el contrato inteligente, de modo que el pago se produce de forma instantánea y autónoma de los jugadores al ganador.

Esta arquitectura ofrece a los jugadores dos protecciones que antes no estaban disponibles en el póker online: la primera, que los jugadores ya no tienen que confiar en un sitio web ni entregarle sus depósitos; la segunda, que

tampoco tienen que confiar a ciegas en la lógica de los juegos. Dicho de otro modo, que los usuarios saben que los operadores no pueden robarles los depósitos ni «mirar» sus cartas.

Más información sobre el impacto de la blockchain en el juego online en <libroblockchain.com/juego/>.

Medios de comunicación y la blockchain

Covadonga Fernández González

Desde el punto de vista del ejercicio de la profesión periodística, el alcance de la incorporación de la blockchain puede considerarse revolucionario, ya que apunta hacia la desintermediación de la misma. Hasta hace muy poco, la imagen de un periodista que no realizara su labor en un medio de comunicación determinado parecía impensable; pero nada es lo que fue. Los bancos trabajan para convertirse en empresas de servicios de software, las compañías tecnológicas para realizar las funciones de los bancos y las de telefonía para transformarse en medios de comunicación y proveedores de identidad.

Plataformas como Steemit,[40] desarrollada con tecnología blockchain, ya recompensa a los periodistas o bloguers con criptomonedas en función de los votos que los lectores conceden a sus contenidos. A su vez, también remunera a los usuarios por votar sus informaciones favoritas. Estamos, pues, ante el abismo del periodismo sin medios. Sólo en España, entre los años 2008 y 2015 cerraron 375 diarios, revistas y demás plataformas de comunicación, y más de 12.000 profesionales perdieron su empleo.[41]

La revolución de internet

Desde la aparición de internet hace veinticinco años, los medios de comunicación han creído que la publicidad huida del formato en papel iría a parar a los sitios web de dichas publicaciones. Y así ha sido, aunque no como ellos pensaban, pues los anunciantes exigieron tarifas infinitamente más bajas por subirse a la red. A esto se suma que el número de potenciales receptores de la tarta de la inversión publicitaria se haya multiplicado casi hasta el infinito. La situación, por tanto, en lugar de arreglarse por sí sola como esperaban los editores, no ha hecho sino deteriorarse aún más. Pero lo peor estaba aún por llegar. En 2004 surgió la Web 2.0 y, con ella, la capacidad de interactuación de los usuarios. Este hecho marca un período de inflexión en la historia de los medios: las wikis, los blogs, las redes sociales como Facebook, y otros descendientes de la denominada Web 2.0 empezaron entonces a dar voraces

dentelladas a una ya mermada tarta de inversión publicitaria. En la actualidad, gigantes como Google y Facebook engullen nada menos que el 75% de la publicidad online.

La industria de los medios ha caído en la trampa de trabajar para engordar a Google, Facebook o Twitter, que han acabado devorándolos. Trabajamos y competimos entre nosotros para obtener la dosis diaria de «me gusta» y la buena posición y referencias que necesitamos para impactar en los lectores, consumidores o telespectadores. Mientras que antes los medios de comunicación eran la única plataforma para estar en la esfera pública, ahora son sólo una más. Pero si todo esto es cierto, no lo es menos también que las redes sociales necesitan del capital simbólico de las cabeceras tradicionales para ganar credibilidad, de ahí los acuerdos que están surgiendo entre ambos mundos. La nueva estrategia de los medios pasa por colaborar y juntarse con las compañías que han irrumpido en su modelo de negocio.

En el tiempo que va desde la aparición de internet, la única industria que ha permanecido fiel a su patrón de negocio ha sido la de los medios. Incluso las webs corporativas de compañías de telefonía, de energía, de organismos y organizaciones internacionales o de entidades financieras se han convertido en excelentes medios de comunicación especializados en contenidos específicos de gran valor, muchos de ellos generados por profesionales ajenos al periodismo.

Axel Springer y Thomson Reuters, dos de los grandes grupos de comunicación del mundo, invierten y trabajan en proyectos relacionados con la blockchain para adaptarse al futuro del internet del valor. La apuesta de Thomson Reuters respecto a la blockchain va más allá de un ámbito de aplicación concreto ligado a los medios de comunicación: a partir del convencimiento de que la información por sí sola ya no es suficiente, lo que hace es vender a sus clientes/asociados/lectores información inteligente que aporta valor. Desde la primavera de 2016, Reuters forma parte de Hyperledger,[42] el proyecto que la Fundación Linux ha puesto en marcha para fomentar el desarrollo de las blockchains privadas en diferentes sectores de la industria y que ya están aplicando importantes multinacionales y entidades bancarias.

Que dos titanes como Axel Springer y Thomson Reuters inviertan y experimenten con la blockchain ratifica la importancia de esta tecnología para explorar nuevas oportunidades de negocio y, también, para intentar resolver la profunda crisis que padece el sector de los medios. La blockchain promete democratizar los mercados aún más que internet y llevarnos a entornos más colaborativos y descentralizados. Y los medios podrían estar ahí, porque todavía tienen margen para actuar y desarrollar su papel institucional como guardianes de información veraz, un derecho irrenunciable de los ciudadanos.

Es en la desintermediación donde el potencial de la tecnología blockchain de Bitcoin podría cambiar el futuro de los medios mediante transacciones inmediatas y sin intermediarios, abriendo una puerta de esperanza a la industria de los medios y también a los profesionales de la información al permitir a los usuarios comprar, por fracciones de euros o bitcoins, artículos, reproducciones de vídeos, noticias, fotos, dibujos, suscripciones al medio por páginas o secciones concretas, minutos de lectura, horas o días. Yendo un poco más allá, cada periodista podría programar sus propios Smart Contracts poniendo las condiciones concretas en las que se consumiría su producto. Es decir, cada periodista podría definir su propio modelo de negocio para editores o consumidores finales.

Micropagos de contenidos y nueva relación de los usuarios con la publicidad de los medios

Axel Springer también participa del capital de SatoshiPay,[43] una startup que en 2016 puso en marcha una plataforma para que los editores web puedan monetizar sus contenidos, ya sea a través de su lectura, su escucha o su visionado. La tecnología de pago de esta empresa permite transferir cantidades tan pequeñas como 0,01 euros, y todo gracias a la blockchain. Esta startup ofrece una alternativa a los editores que desean llegar a esos consumidores que han instalado bloqueadores de publicidad, al facilitarles poder fragmentar la relación con el soporte, ofertando una sección o producto determinados.

Además, se ha demostrado que gestionar los contenidos como si fuesen canciones o videojuegos puede funcionar. Según PageFair,[44] una empresa que ofrece soluciones para contrarrestar el bloqueo de anuncios, más de 198 millones de personas utilizan bloqueadores publicitarios, práctica esta que

genera a los editores online pérdidas superiores a los 22.000 millones de dólares. La respuesta de los distribuidores de contenidos ante la temida presencia de los bloqueadores de publicidad ha sido bloquear, a su vez, el acceso a estos usuarios a la lectura completa del producto, invitándolos, para solucionar esta situación, a desactivar el bloqueador de publicidad. Esta manera de proceder termina provocando la huida de los usuarios hacia webs con contenidos totalmente abiertos. Pues bien, la startup de origen holandés Blendle,[45] que cuenta con el respaldo del diario *The New York Times* y Axel Springer, ha conseguido en dos años que alrededor de 200.000 usuarios paguen por leer contenidos sin necesidad de suscribirse al medio ni consumir publicidad no deseada.

La blockchain también es capaz de desintermediar la publicidad online y conectar a los consumidores directamente con las marcas y los medios. Y también puede resultar eficaz para la preservación de la privacidad, algo que el duopolio publicitario Facebook/Google imposibilita, porque los datos que dejan en ellas los usuarios —desde el rostro al lugar de residencia— son el corazón de su negocio. Por ejemplo, la aplicación Unonimity[46] permite el acceso libre a cualquier medio a cambio de ver anuncios personalizados, pero sin tener que dejar huellas de datos personales. Unonimity, que recompensa a los receptores de anuncios, explica que ellos nunca sabrán el nombre del usuario, correo electrónico, número de teléfono, dirección o cualquier otra forma de identidad. Tampoco conocerán nunca quiénes son los amigos de los consumidores, ni les solicitará información bancaria o tarjeta de crédito, ni información sobre género, raza, edad, orientación sexual o estado civil. Esto supone intentar contrarrestar el poder de Google y Facebook en la lucha por la inversión publicitaria, ya que ofrece al receptor de la misma unas condiciones más favorables.

En el ámbito de la publicidad, la herramienta blockchain que más controversia ha generado en el mundo editorial es el buscador Brave,[47] cuya principal característica es que permite ver contenidos sin publicidad distribuyendo bitcoins a las webs de contenidos desde el navegador del lector según el tiempo que dedica a cada página. Pese a que los responsables de algunas de las cabeceras de periódicos más importantes, como *The New York Times* o *The Washington Post*, enviaron una carta al consejero delegado de Brave, Brendan Eich, anterior consejero delegado de Mozilla y gestor del

navegador Firefox, en la que lo acusaban de robar sus contenidos en beneficio propio, la plataforma ha anunciado que los editores recibirán el 55% de los ingresos. Lo más polémico de este buscador es que una de las opciones que ofrece al usuario es ver anuncios contratados directamente por Brave, prometiendo una navegación más rápida y el respeto de la privacidad.

Cambio en las posibilidades del ejercicio profesional

La libertad de prensa, que es uno de los núcleos de las sociedades democráticas, no ha encontrado aún su total protección en internet. En algunos países con Gobiernos autoritarios, tanto los periodistas, como incluso los editores o los receptores de la información, se ven amenazados por las huellas que dejan las publicaciones. Aquí la capacidad de desintermediación de la blockchain da un paso más, ya que permite también garantizar el anonimato de los primeros y los últimos, mientras que, al mismo tiempo, facilita la financiación de los profesionales. Es lo que están desarrollando tres periodistas holandeses en Publicism, un proyecto con apoyo de las instituciones profesionales de los Países Bajos,[48] o la empresa de protocolos abiertos Blockstack.

Al igual que en otros sectores, como el agrícola o el de los productos de lujo, la blockchain también puede utilizarse para conocer la trazabilidad de un determinado contenido. Es decir, saber en cada momento los ingresos que genera cada contenido, en función del número de visionados o recepciones, y qué soportes lo han publicado. Esto también entraña sus peligros, pues los periodistas pueden verse compitiendo, para sobrevivir, con contenidos que saben de antemano que tendrán un reconocimiento popular.

Desde la misma lógica de la trazabilidad, con la blockchain puede conocerse el origen de las noticias que, después, se constatan falsas. Un origen que, en la medida de la defensa del anonimato que permite la propia blockchain, puede ser anónimo. Ahí ha de estar la profesionalidad de los periodistas para dar credibilidad o comprobar las informaciones que reciben y difunden.

Más información sobre el impacto de la blockchain para los medios de comunicación en <libroblockchain.com/medios/>.

Las ONG y la blockchain

Íñigo Molero Manglano

Existe un tercer sector que toma elementos de los dos primeros, el público y el privado, pero que mantiene indemne su peculiar singularidad sea cual sea la forma jurídica que adopten los entes que lo componen: la ausencia de ánimo de lucro en el desempeño de sus labores. Se trata de un sector que surge para suplir las deficiencias del Estado en la gestión de cuestiones de índole social, cultural o medioambiental, por citar sólo algunos ejemplos. Así, bajo el amparo de la ley, se constituyen diversos entes que adoptan una forma jurídica concreta en función de sus fines y necesidades: asociaciones de afectados, organizaciones no gubernamentales (ONG), plataformas de voluntariado, cooperativas, mutualidades, fundaciones… En lo que todos estos entes coinciden es en su carácter privado, autónomo (es decir, independiente del Estado y soberano en sus decisiones) y sin ánimo de lucro, sin olvidar su apuesta por el voluntariado.

Por su propia idiosincrasia, este tercer sector adopta procedimientos propios de las empresas privadas al uso, como pueden ser, además de la mencionada forma jurídica, los órganos de gobierno, las responsabilidades de los directivos o un modelo similar de gestión. Este último implica desarrollar estructuras y estrategias comerciales, aprovisionamientos de fondos y demás recursos necesarios para desarrollar sus actividades y lograr el fin perseguido. Hay, sin embargo, una diferencia fundamental con la empresa privada, y es que el modelo de elección de los mandos que rige aquí no proviene de ese sector privado, sino del público. Esto significa que los representantes deben ser elegidos de forma democrática entre todos los miembros asociados, y en este sentido es habitual la celebración de asambleas generales —ordinarias o extraordinarias— como órgano de expresión popular de todos los miembros.

Estas singularidades descritas llevan implícitas que todas las posibles aplicaciones desarrolladas tanto para el sector público como para el privado, sean también susceptibles de incorporarse al tercer sector que, además, puede desarrollar otras propias, como a continuación veremos.

Una nueva forma de financiación para las ONG: las

criptomonedas

La aparición de la tecnología blockchain en 2009, inauguró la posibilidad de recibir donaciones en criptomonedas. «Algo», en realidad, que muy poquitos sabían muy bien qué era y para qué servía realmente. Sin embargo, el paulatino interés por el bitcoin y otras criptomonedas posteriores, «confirieron» valor económico a ese «algo» que bien podía convertirse en dinero de curso legal o intercambiarse por bienes y servicios. Se creó así una inercia guiada por el pragmatismo que suele regir en estos entes, de modo que organizaciones como Save the Children, Wikileaks o United Way —la mayor asociación caritativa en Estados Unidos— comenzaron a aceptar criptomonedas como forma de financiación. Esta lista está en constante actualización. También en España encontramos a la Asociación de Ayuda a las Víctimas del 11-M, pionera en desarrollar proyectos europeos y redes transnacionales asociativas. Así que el primer contacto de este tercer sector con la tecnología blockchain ha tenido que ver con donaciones, sobre todo en bitcoins.

El papel de las criptomonedas, sin embargo, va más allá. Por su diseño y estructura, este medio digital de intercambio suponía una mejora respecto a los procedimientos habituales de recibir aportaciones dinerarias, periódicas o puntuales, de colaboradores y afiliados. Con el sistema bancario al uso, algo en principio tan básico como transferir pequeñas cantidades de dinero (de 1 euro o 2 euros) o domiciliar pagos mensuales es una batalla perdida de antemano. La ausencia de interés práctico se sustenta en un argumento entendible: al donante le «duele» que un porcentaje insultante del dinero donado (hasta el 80%) se lo queden los intermediarios. Con la tecnología blockchain, en cambio, es posible realizar microdonaciones desde un dispositivo móvil desde cualquier lugar y a cualquier hora, siempre que se tenga conexión a internet, y ello sin que los intermediarios se queden con parte del dinero. Así lo puso de manifiesto ChangeTip, una aplicación hoy ya desaparecida del ecosistema blockchain que operaba a través de redes sociales como Twitter. En la actualidad encontramos BitGive, una ONG especializada en bitcoins, y su plataforma de blockchain pública GiveTrack, creada para canalizar donaciones transparentes y financiar proyectos. Se trata de uno de los proyectos más destacables en el mundo de las

ONG y la blockchain porque cualquier usuario se puede incorporar y apoyar el proyecto que más le guste y, a partir de ahí, realizar un seguimiento real y actualizado del recorrido del dinero hasta su destino final.

Transparencia: un valor clave para las ONG

La financiación de la que se nutren las ONG viene dada tanto por el sector público (a través de subvenciones) como por el privado. Para conseguir financiación pública es necesario presentar proyectos que detallen la finalidad y propósito del dinero solicitado y, si éste se logra, hay que acreditar los gastos ejecutados en una memoria técnica justificativa. En cambio, en la financiación privada no existe un procedimiento tan regulado, pues son las propias partes las que suelen acordar convenios de colaboración bilaterales.

Gracias a la blockchain cualquier patrocinador, sea anónimo, público o privado, puede seguir el recorrido realizado por su donación o subvención a lo largo de toda la cadena de suministros y en cualquier momento. Por eso, y aunque sólo sea porque una mala gestión podrá ser puesta en evidencia con absoluta certeza, el uso de esta tecnología favorecerá las buenas prácticas y la moderación y prudencia en el manejo de los recursos. Prácticas como la corrupción, la gestión inapropiada o la mala praxis tendrían difícil cabida en una ONG que lograra integrar con éxito una plataforma blockchain en el desarrollo de su actividad.

Por otro lado, todas las decisiones adoptadas por la junta directiva o las correspondientes asambleas quedan registradas en la blockchain. El escéptico dirá que esto no supone innovación alguna, ya que esa información suele estar disponible en la página web o en las oficinas de la ONG, a disposición de cualquier asociado que lo solicite. Y es cierto. Pero no lo es menos que con la blockchain esa información se obtiene de forma veraz y actualizada, sin necesidad de depender de un tercer ente de confianza, como son los mandos de la organización.

Colaboraciones internacionales de las ONG

Al igual que una gran empresa privada o un organismo público, cualquier ente del tercer sector puede constituir una blockchain privada para optimizar sus procedimientos de gestión. Esta posibilidad adquiere sentido para aquellas

asociaciones que manejan datos o información confidencial de sus usuarios, algunos de los cuales tienen además una protección jurídica reforzada. Es el caso, por ejemplo, de víctimas de delito que estén siendo atendidas en asociaciones creadas al efecto. Con la blockchain tendrían la seguridad de que sus datos íntimos y personales no pueden ser robados de la base de datos de la organización. Para aquellas grandes estructuras asociativas, que además tienen vocación y ámbito de actuación internacional, la blockchain debe ser una solución a tomar necesariamente en cuenta. Además, distintas blockchains privadas podrían interrelacionarse entre ellas, lo mismo que con otra pública creada para dar solución a un problema concreto, por ejemplo una catástrofe humanitaria que precisara de ayuda inmediata y cooperación internacional. Una blockchain construida al efecto para canalizar todos estos esfuerzos sería una respuesta perfecta, pues en ella, y de forma automatizada, podrían registrarse las necesidades urgentes y aquellas otras ineludibles a medio y largo plazo.

Pero la blockchain no se reduce a un caso concreto con un límite temporal, como puede ser una catástrofe humanitaria, sino que puede adoptar también un carácter indefinido y establecer cooperaciones segmentadas según el ámbito de actuación: ayuda a la infancia, lucha contra el hambre, atención sanitaria, víctimas del terrorismo, ecología… De este modo se podrían establecer relaciones con otras iniciativas que surgieran en ámbitos privados, auspiciados en un nuevo y renovado concepto de responsabilidad social corporativa (RSC).

Desarrollar algunas de estas posibilidades es uno de los objetivos de Start Network, una red de asociaciones del tercer sector que en abril de 2016 anunció el lanzamiento, de la mano de la empresa de blockchain ConsenSys, de un proyecto piloto para explorar aplicaciones sustentadas en la plataforma blockchain de Ethereum. Sobre este protocolo puede tomar forma cualquier contrato inteligente o Smart Contract.

Por otro lado, el tercer sector tampoco es ajeno a las posibilidades de financiación que brinda el crowdfunding. Un ejemplo de esto lo hallamos en los contratos condicionados: un patrocinador compromete cierta cantidad de dinero para desarrollar un proyecto; según el protocolo establecido, si en el tiempo estipulado en el contrato no se ha llegado a recaudar el dinero mínimo necesario para desarrollar la actividad prevista, ésta se cancela. Un Smart Contract podría revertir automáticamente, sin necesidad de intervención humana ni de dar

explicaciones, todas las cantidades donadas a los patrocinadores originales. Otra propuesta viene de la italiana Helperbit, que, a través de una relación directa entre donantes y donados, y utilizando monedas locales o bitcoins, pretende eliminar intermediarios a la hora de recibir donaciones.

La adopción de la blockchain en el tercer sector lleva también un último valor añadido: la imagen. Entre dos organizaciones distintas que realizan tareas similares, la implementación por parte de una de ellas de una blockchain puede ser un elemento determinante para nuestra elección, simplemente porque en ella no se da esa entidad central que supervisa todo el proceso y que, caso de no estar a la altura o de ceder a malas prácticas, puede conducirlo a la ruina. Así que lo que hoy constituye una posibilidad deseable, mañana puede llegar a ser una exigencia más que comprensible.

Más información sobre el impacto de la blockchain para las ONG en <libroblockchain.com/ong/>.

El sector público y el uso de la blockchain

Roberto Fernández Hergueta

La relevancia e importancia de la administración pública es superior a cualquier otro sector económico, organización o movimiento social. De hecho, desde el punto de vista económico, representa casi el 45% del total del producto interior bruto (PIB) español. Y no sólo eso: es también el responsable de asegurar el crecimiento sostenido y estable de una nación, aumentar el bienestar de sus ciudadanos e impulsar medidas que favorezcan la creación de empleo de calidad y una mejor redistribución de la renta y de la riqueza disponibles. La blockchain podría ser uno de los instrumentos imprescindibles para lograr estos objetivos, y ya hay países adelantados que están explorando esta posibilidad.

La administración está en plena crisis de identidad y necesita identificar su verdadero rol. Entre otros, su papel como regulador, que debería ser un modelo no intrusivo, inteligente y proactivo como defensor de libertades y garante de la igualdad de oportunidades. El establecimiento del entorno regulatorio debe facilitar los negocios y garantizar un ambiente propicio para su desarrollo o, al menos, no poner trabas innecesarias. Mas, por lo general, los líderes de los Gobiernos y las administraciones públicas no están preparados para afrontar los desafíos del siglo XXI.

Un nuevo modelo de administración pública

El primer paso para resolver un problema es identificarlo. En este caso, ese problema no es otro que la certeza de que los modelos tradicionales son incapaces de dar respuestas integrales a las demandas de la sociedad de hoy. Es necesario incorporar nuevas perspectivas, superar las diferencias, aunar esfuerzos, espolear la conciencia crítica y recuperar la confianza.

Los ciudadanos exigimos simplicidad, ubicuidad e inmediatez; demandamos un nuevo modelo de administración pública, más transparente, más rápido, más eficiente y más integrado en la vida diaria de la ciudadanía. Y no sólo esto, sino que también queremos participar en aquello que nos interesa.[49] Una administración incorporada al cambio tecnológico que representa

la blockchain haría posible estas demandas al propiciar que los ciudadanos, pero también las empresas y organizaciones de la sociedad civil, puedan acceder a información relevante, mejorar los servicios públicos y participar en la toma de decisiones de manera más activa. La transparencia, la confianza, la ética y la empatía son elementos clave que buscan los ciudadanos en el nuevo modelo de Gobierno y administración pública.

Hasta el momento se han lanzado numerosas iniciativas orientadas a la digitalización (es decir, al uso de tecnología para automatizar y optimizar los procesos actuales de negocio), pero digitalizar no significa transformar. Transformar es repensar los procesos reales operativos en un mundo que ya es digital y donde ya está integrado el ciudadano. Ahí es donde la tecnología blockchain puede aportar soluciones.

La nueva realidad del mundo descentralizado en el área de Gobierno

Los modelos de conceptualización digital basados en el diseño estratégico y la tecnología blockchain[50] son uno de los elementos clave para la generación de un nuevo tipo de administración descentralizado. Para entender esto de forma más concreta vamos a presentar a continuación algunos casos de aplicaciones potenciales en países que ya están explorando el uso de la tecnología blockchain y su capacidad para generar un mundo más equilibrado, democrático y sin la necesidad de intervención de terceras partes.

Una de esas aplicaciones se refiere a los registros, tanto públicos como privados, que gracias a la tecnología blockchain pueden ser descentralizados. En el caso de los registros públicos tenemos el registro de títulos de la propiedad, el de vehículos, las licencias de negocio, el censo poblacional, los registros criminales, los pasaportes, los certificados de nacimiento, los certificados de defunción, los procesos electorales o los sistemas de voto.[51] Esta categoría puede hacerse extensible a otras tipologías de permisos, por ejemplo, las subvenciones otorgadas. A nivel de registros privados existen aplicaciones en los registros médicos y educativos, en la gestión de becas, el arbitraje, las patentes, los registros de apuestas, las donaciones, etcétera.

Gracias al uso de la tecnología blockchain serán posibles la gestión de residuos, el alumbrado público, el agua, los jardines públicos, los parques o los modelos de pago de impuestos por uso de servicios. Igualmente, se podrán crear activos digitales de la administración que permitan nuevas formas de uso, mantenimiento y reparación. Los Gobiernos incluso podrán explorar nuevos modelos de identidad digital, modelos descentralizados orientados al empoderamiento de los ciudadanos o a redefinir los sistemas de justicia, sanidad, educación y hacienda.

Gobiernos pioneros en el uso de la tecnología blockchain

A pesar de la resistencia propia del sector público a los grandes cambios y su tendencia a aguardar un caso de éxito concreto que sea fácilmente replicable, en la actualidad son varios los proyectos piloto de blockchain en curso en todo el mundo. Y la cifra no deja de crecer cada día que pasa.

La sociedad digital más avanzada del mundo y, por tanto, la vanguardia en el ámbito de la blockchain es sin duda Estonia. Este pequeño país báltico emplea esta tecnología en sus registros fiscales y empresariales, y de ahí la ha extendido a los registros sanitarios electrónicos de sus ciudadanos para protegerlos. El Reino Unido, en cambio, explora el uso de la blockchain para pagar y monitorizar becas de investigación. Con anterioridad, el Gobierno había realizado una prueba de concepto con las personas que reciben pago de asistencia social. Los resultados de la prueba piloto[52] fueron tan exitosos, que se decidió que la blockchain fuera la tecnología aplicable a todo el sector del bienestar social.

En Australia, se investiga el uso de la blockchain en casos relacionados con las comunicaciones gubernamentales, la seguridad cibernética y la logística. También en materia de seguridad pública: así, el Gobierno ha establecido que los vídeos filmados por la policía se almacenen en una cadena de bloques para garantizar que no se han alterado. Además, se está estudiando emplear esta tecnología en la monitorización del uso correcto de los fondos públicos que el Gobierno federal destina a los gobiernos locales. La seguridad alimentaria (certificado en origen) y los procesos electorales son otros campos en los que se valoran las posibilidades de la blockchain.

En Singapur se está desarrollando una aplicación para combatir el fraude detectado en las relaciones entre comerciantes y bancos. Los defraudadores se valían de facturas duplicadas, con las cuales obtenían indebidamente cientos de millones de dólares de los bancos. El Gobierno tomó cartas en el asunto y desarrolló con los bancos locales un sistema basado en una cadena de bloques con un hash criptográfico único de cada factura. Los bancos comparten esta clave única, en lugar de los datos en bruto, y si otro banco intenta registrar una factura con los mismos detalles, el sistema es alertado.

En 2020,[53] Dubái tiene previsto trasladar todos sus documentos a una blockchain y no volver a emplear papel. Hasta entonces calcula liberar 25 millones de horas de productividad anuales destinadas a la gestión de los documentos guardados. El Gobierno ha identificado además otros seis proyectos piloto para el uso de la blockchain: registros de salud, comercio de diamantes, registro de transferencias de títulos, registro de empresas, testamentos digitales e impulso del turismo. Y en Georgia, Ghana, Honduras, Rusia y Suecia se han explorado también proyectos con diferentes tecnologías para registrar títulos de propiedad que se encuentran en fase de prototipo.

Todo esto confirma que la administración pública podría ser uno de los grandes beneficiarios de la revolución blockchain y, por extensión, los ciudadanos, que gracias a estas iniciativas verían elevada su calidad de vida y condición ciudadana.

Más información sobre el impacto de la blockchain en el sector público en <libroblockchain.com/sector-publico/>.

Capítulo 3

Modelos de uso sectorial de la blockchain

Las compañías que ya disponen de un exitoso modelo de negocio buscan mejorarlo recurriendo a las blockchains privadas o híbridas. Las blockchains públicas, en cambio, parecen centradas en solucionar las necesidades transversales implícitas en el mundo digital, como pueden ser el comercio electrónico, la identidad digital, los medios digitales (música, vídeo e imágenes) y el propio internet de la información.

En el mundo de las blockchains las posiciones ideológicas pueden ser muy dispares. En un extremo se dan posicionamientos derivados del movimiento original de la blockchain pública que son extremadamente progresistas, cuando no libertarios y con propuestas osadas e inconformistas que rayan lo antisistema. En el opuesto, encontramos el mundo de las blockchains privadas, que en muchos casos representa la manera más formal y tradicional de entender los negocios. Y entre unos y otros se sitúa una miríada de posturas intermedias, impregnadas de pragmatismo y sentido común, que apuestan por proyectos estables en el tiempo. Independientemente de las preferencias o afinidades ideológicas, el reto para cualquier directivo, empresario o startup es entender el conjunto de soluciones propuestas para una optimización del mercado.

Con los ejemplos que siguen a continuación esperamos dar una imagen global que hallará complemento en el siguiente capítulo, dedicado a soluciones transversales.

Participación ciudadana y voto electrónico

Óscar Lage Serrano

La diversidad política, social y económica de las sociedades actuales desborda los esquemas tradicionales de gobernanza y pone de manifiesto la limitada capacidad de éstas para ofrecer respuestas efectivas a los nuevos problemas y demandas. Éstos precisan de una acción colectiva y de diagnósticos compartidos para su solución. Sólo una vez abordado con éxito este debate es posible plantear un horizonte de objetivos e intervenciones jerarquizadas y progresivas, igualmente compartidas por todas las partes. La participación ciudadana y la exigencia de transparencia, tanto del Gobierno como de cualquier organización en general, son dos fenómenos que ya se están dando a nivel mundial y en los que la situación económica y política actúa como catalizador.

Resultado de ello es el nuevo paradigma de Gobierno abierto, cuyos ejes fundamentales son la rendición de cuentas y la transparencia en la gestión, el fomento de la participación y la colaboración de la ciudadanía en el diseño y ejecución de las políticas. Se trata de un movimiento que, tras irrumpir con fuerza, se ha afianzado como una revolución en el conocimiento y la comunicación en nuestra sociedad actual, así como en el propio concepto de lo que hasta ahora conocíamos por democracia.

Los procesos participativos y el voto electrónico

La participación ciudadana es ya una realidad en diferentes países y administraciones locales. Estas primeras prácticas están siendo acogidas con gran éxito, tanto por la ciudadanía como por los propios órganos de gobierno. No obstante, y dado que existe una gran desconfianza tanto en lo que se refiere a la seguridad como a la privacidad del voto, por lo general estas experiencias no son vinculantes.

Por otro lado, países europeos como Estonia y Suiza utilizan ya el voto online, que ha tenido una especial acogida entre los ciudadanos residentes en el extranjero. Conviene, sin embargo, ser cautos, pues expertos como Jason Kitcat[54] manifiestan que en el primero de esos Estados se han observado

diferentes maneras de alterar los resultados. Es por ello que países como Dinamarca, Francia, el Reino Unido u Holanda, fuera de algunas pequeñas pruebas, no se han atrevido a aplicarlo aún en el conjunto de sus territorios. Ese miedo y desconfianza generalizada de la ciudadanía en las tecnologías utilizadas en la actualidad —alentada también por expertos como Bruce Schneier—[55] es lo que está frenando el despliegue del voto online, un sistema que podría ofrecer un gran valor a todas las partes e incluso reducir muy significativamente los costes de unas elecciones.

Los expertos consideran que el voto online debería garantizar:

- Una autenticación fuerte para ratificar la identidad del votante.
- El anonimato, de cara a que ninguna persona que pueda tener el control de la plataforma obtenga la trazabilidad del voto.
- La auditabilidad, tanto del propio proceso (a través de un recuento o análisis del proceso) como de la plataforma de gestión (muchos expertos recomiendan el uso de sistemas de código abierto).
- La inalterabilidad del voto, es decir, no permitir que se pueda modificar la intención de ningún voto bajo ningún concepto.

Beneficios de la blockchain en el voto electrónico

El carácter descentralizado de la blockchain permite dar respuesta a una de las mayores deficiencias de las plataformas actuales, que al estar basadas en sistemas centralizados y gobernados por una única fuente no garantizan la inalterabilidad de la intención del voto, por lo que cualquier manipulación en la base de datos podría suponer un cambio drástico en los resultados de una votación online. En un sistema así es obligado que todas las partes confíen en el administrador central. En cambio, la blockchain lo que hace es descentralizar dicha responsabilidad y dispersarla entre todos los nodos participantes, que son los que logran el consenso sobre los datos albergados en la base de datos.

A esta gran ventaja hay que sumar otra: la auditabilidad que la blockchain ofrece frente a los sistemas tradicionales. Gracias a esta tecnología sería posible incluir nodos públicos, nodos de auditores e incluso nodos de medios de

comunicación, que podrían auditar todo el proceso y, si la regulación lo permite, comunicar los resultados del mismo en tiempo real a los interesados —ciudadanos o asociados— sin que ello comprometa la seguridad del sistema.

Todo ello, sumado al anonimato que ofrece por diseño, postula a la blockchain como la tecnología base de la participación y votación online del futuro.

Más información sobre participación ciudadana y voto electrónico con la blockchain en <libroblockchain.com/voto/>.

Smart Cities en la era blockchain

Stefan Junestrand

La Ciudad Inteligente es un concepto que hace referencia al uso de las TIC en la gestión de los servicios urbanos para optimizar aspectos como eficiencia, accesibilidad, seguridad, medioambiente, participación ciudadana o economía. El gran interés por las Ciudades Inteligentes es especialmente intenso debido a una serie de tendencias socioculturales, tecnológicas y económicas confluentes y en las que la tecnología blockchain puede tener un destacado protagonismo.

Nuestro punto de partida son las mismas ciudades, que atraen a una cada vez mayor parte de la población. En el año 2014, el 54 % de la población mundial estaba ubicado en áreas urbanas, un porcentaje que está en continuo crecimiento y que se espera que para 2050 alcance el 66 %. Y aunque las ciudades cada vez generan una mayor parte de la economía y bienestar de las naciones, también son el foco principal de problemas administrativos, organizativos, logísticos, sociales o medioambientales.

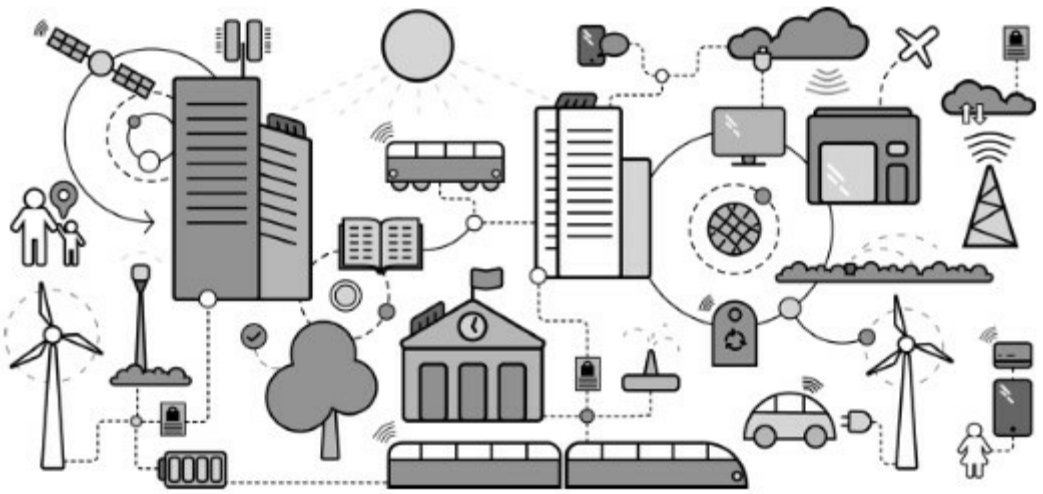
Un aspecto clave para entender las ciudades inteligentes es el fuerte impacto que han tenido las TIC y que se traducido en un tipo de sociedad nueva, la sociedad de la información.[56] Internet y el internet de las cosas (IoT) nos han llevado a ser una sociedad digitalizada e hiperconectada, tanto entre personas como entre máquinas. Y otras tecnologías, como la inteligencia artificial y la robótica, que hace sólo unos pocos años sonaban más a ciencia ficción que a otra cosa, empiezan ya a formar una parte real de nuestras vidas.

No hay que descartar tampoco la influencia de nuevas tendencias sociales que demandan, cada vez más, una mayor eficiencia administrativa y modelos más directos de participación ciudadana, además de mayor transparencia y más acceso a la información pública. Esto, junto con el desarrollo del Big Data, Open Data, etc., está transformando la administración pública y la manera en la que se prestan los servicios y se ofrece el acceso a la información.

Pero lo que convierte la ciudad inteligente en un entorno realmente único es que se trata de un sistema transversal que une un gran número de servicios verticales de características muy distintas. Ejemplo de ello es la competencia de

las administraciones públicas en materias como la gobernanza, economía, asuntos sociales, movilidad, seguridad, energía, cultura y medioambiente. Todos estos servicios son susceptibles de modernizarse con el uso de la tecnología, pero el hecho de poder integrarlos horizontalmente, bajo un sistema único que hable el mismo lenguaje, será la gran revolución de las Smart Cities. Para que esta integración se produzca es necesaria una plataforma segura, transparente y con un lenguaje y unas reglas comunes, características todas ellas que cumple la blockchain y que podrían hacer de ella la «columna vertebral» tecnológica para el intercambio de la información en las ciudades inteligentes.

Modelo interconectado de una ciudad inteligente con tecnología blockchain.



Este desarrollo hacia ciudades realmente inteligentes supone, además, una gran oportunidad para optimizar su organización y gestión, y hacer que éstas estén al servicio de los ciudadanos. Blockchain puede jugar un papel clave en este proceso, no solamente debido a toda la gama de innovaciones tecnológicas que conlleva, sino también por su modelo económico distribuido, su robustez y transparencia.[57] Las más de doscientas ciudades inteligentes[58] impulsadas en China, así como las más de cien del proyecto Smart Cities Mission de la India,[59] sin olvidar el Smart Cities Initiative de Estados Unidos,[60] el Plan Nacional de Ciudades Inteligentes de España[61] o el Smart Nation de Singapur,[62] demuestran que la apuesta por estas urbes es hoy ya una realidad.

La blockchain como plataforma para las ciudades inteligentes

Un reto único para las Smart Cities a nivel tecnológico, es la necesidad de

interconectar los distintos servicios «verticales» de la ciudad bajo una misma Plataforma Tecnológica de Ciudades Inteligentes. Se establece, así, una interconexión «horizontal» capaz de integrar todos estos servicios verticales. Para visualizar las grandes ventajas de esta posibilidad y sus implicaciones sobre la gestión actual, sólo hay que pensar en casos donde la coordinación entre las diferentes áreas y actores son imprescindibles para lograr el fin deseado. Esta integración minimizaría tiempos de respuesta de ejecución y simplificaría la duplicidad de las tareas compartidas en varias de estas áreas. Como ejemplo podemos citar la gestión de grandes eventos municipales o la intervención de los servicios de emergencia. Dos acciones que implican la participación de diferentes áreas de servicios de la ciudad que optimizarían relaciones y procedimientos bajo esta plataforma «horizontal». Además, esta plataforma tecnológica horizontal puede ser también la base del desarrollo de muchos nuevos servicios generados sobre información transversal, así como de iniciativas tanto públicas como de la empresa privada.

Este tipo de plataformas para la integración de servicios ya existen. A nivel público, la más conocida e interesante desde el punto de vista de la blockchain es FIWARE:[63] impulsada por la Unión Europea, su comunidad, abierta e independiente, tiene como objetivo «construir aplicaciones inteligentes en ecosistemas abiertos y sostenibles de software en múltiples sectores». Cerca de un centenar de ciudades del mundo utilizan ya FIWARE para sus plataformas de las Smart Cities. A su amparo han surgido iniciativas como el FIWARE Lab,[64] un entorno *sandbox* centrado en soluciones de Open Data para ciudades y otras organizaciones. En la actualidad, se experimenta también en cómo integrar la tecnología blockchain en las aplicaciones de ciudades inteligentes[65] con el aval de una plataforma no jerárquica, pública y segura.

A continuación, analizaremos algunas de las principales áreas de servicios verticales de las ciudades, teniendo en mente la integración de estos servicios con otros en una plataforma horizontal.

Gobernanza y administración pública

A nivel municipal, la mejora de los servicios públicos, la lucha contra la corrupción y una relación con la ciudadanía más participativa, interactiva y democrática son los grandes retos a los que se enfrentan las ciudades. Dado que

se trata de temas que demandan una alta frecuencia de registros y documentación, la transparencia y la seguridad son imprescindibles,[66] y eso es precisamente lo que proporciona una tecnología como la blockchain: una plataforma de información neutral, no jerárquica, accesible y segura. Otra ventaja es que con un registro blockchain es posible interconectar de forma natural registros administrativos (leyes, gastos, ingresos, contratos, permisos, propiedades, etc.) que corresponden a diferentes áreas de servicios. El valor de la interconexión transversal de los servicios queda así garantizado también.

Urbanismo y espacio público

La digitalización de las herramientas tradicionales del urbanismo, como pueden ser las normativas, planos y mapas, es ya una realidad en la mayoría de ayuntamientos. Pero en la planificación y diseño de las ciudades estamos en estos momentos asistiendo al siguiente cambio: la digitalización total de la información espacial, tanto del territorio como de las infraestructuras y la edificación; es decir, una representación tridimensional exacta de la ciudad, incluyendo las propiedades de los distintos elementos y objetos.[67] Al tratarse de información digital que continuamente se actualiza, lo deseable sería que estos sistemas fueran más abiertos, distribuidos y descentralizados, de forma que cualquier ciudadano pudiera consultar información sobre los espacios públicos (calles, plazas o parques) en relación con su diseño, materiales, fechas y actividades de obras, contratos de mantenimiento, etc., y lo mismo profesionales como arquitectos e ingenieros, que tendrían así a su disposición un modelo tridimensional sobre el que trabajar que les evitaría cualquier error de posición, medición o edificabilidad. Una plataforma de tipo blockchain permite todo esto.

Movilidad sostenible

Es necesario buscar un nuevo modelo de movilidad que reduzca las congestiones de las infraestructuras, aumente la accesibilidad y la seguridad, y tenga un menor impacto medioambiental. A día de hoy ya se están llevando a cabo acciones en este sentido, como la automatización y control de las infraestructuras, la potenciación del uso de vehículos eléctricos y la priorización del transporte público. Pero para que esta transformación tenga realmente un efecto disruptivo es necesario que se base en un sistema abierto, transversal y capaz de compartir los datos y la información en tiempo real, no sólo con los

otros sistemas de movilidad, sino con cualquier usuario o sistema de la ciudad. La blockchain podría ofrecer esa base a través de la cual gestionar el control de acceso a la ciudad[68] o a zonas específicas dentro de la misma,[69] el pago digital en el transporte público[70] y los servicios de uso temporal de vehículos (*carsharing*)[71] o de alquiler de bicicletas.

Seguridad ciudadana

Existen soluciones tecnológicas cada vez más precisas, funcionales y robustas que pueden proporcionar grandes mejoras en la seguridad ciudadana e, incluso, aportarle una nueva dimensión gracias al uso del Big Data y la inteligencia artificial. Así, mediante el análisis de imágenes y patrones de comportamiento es posible no sólo registrar, sino también prevenir ataques, robos y accidentes.

Para evitar el mal uso, o el abuso, de la información recogida, estas soluciones y sistemas deben necesariamente implementarse en concordancia con las leyes y normativas establecidas, como la privacidad de cada persona. Con la blockchain es posible diseñar soluciones en esta vía y que garanticen la seguridad y transparencia de los registros y su documentación.

Economía circular

La estrategia dominante para reducir el impacto medioambiental y económico en la ciudad es la llamada «economía circular».[72] Su objeto es reducir tanto la entrada de materiales como la producción de desechos en el área urbana. En cuanto a los primeros, hay dos tipos de flujos materiales: los «nutrientes biológicos», diseñados para reintroducirse en la biosfera sin perjuicio para el medioambiente, y los «nutrientes técnicos», que no vuelven a la biosfera sino que están concebidos para circular en el sistema de producción. Dentro del ciclo de los «nutrientes biológicos» (como la leche o una lechuga) hay que hacer un seguimiento de sus embalajes a lo largo de la cadena de valor, mientras que en el de los «nutrientes técnicos» (como electrodomésticos y ropa) lo ideal es hacer un seguimiento de su vida útil. Para ello, y gracias a la blockchain, es posible elaborar un registro público y transparente de los datos que no sólo permitiría cobrar tasas por la generación y recogida de diferentes residuos, sino también recompensar el buen hacer de los ciudadanos que menos residuos generen o mejor reciclen.

Edificios

Los edificios son responsables del 40% del consumo energético y del 30 % de las emisiones de CO_2 a la atmósfera. A partir del año 2020, todos los edificios rehabilitados o de nueva construcción tienen que tener la categoría de Edificios de Consumo de Energía Casi Nulo,[73] lo que significa que la energía que consumen tiene que ser renovable y generada de forma local. Una obligación esta que, en combinación con las futuras medidas para disminuir el consumo energético de los edificios en general y la introducción de energías renovables, ofrece nuevas oportunidades energéticas que operen integradas en redes eléctricas inteligentes.[74]

Agua

Aunque en la actualidad ya se utilizan las TIC en muchas redes de suministro de agua, una más detallada medición de los ciclos del agua (desde las fuentes hasta el consumo, pasando por la recogida, el abastecimiento y la depuración) permitiría mejorar la gestión actual. Gracias a la tecnología blockchain no sólo es posible proporcionar una información más exacta, transparente y segura, sino también facilitar la localización de las pérdidas o cobrar en función del suministro exacto consumido, optimizaciones que cobran especial valor en áreas que sufren carencias de agua y restricciones al consumo.

Aire

Reducir las emisiones de CO_2 y controlar las partículas peligrosas en el aire son asuntos clave para el bienestar de la población. La tecnología y, sobre todo, el internet de las cosas juegan un papel clave en el registro, monitorización y seguimiento de los parámetros ambientales. La blockchain puede ofrecer datos abiertos y seguros que alerten sobre altas temperaturas, contaminación o niveles de polen para alérgicos u otros grupos especialmente sensibles, a la vez que informen sobre las zonas en las que se superan los límites de contaminación establecidos.

Parques y jardines

El bienestar y la salud de los parques y jardines es algo que afecta a todos los que viven en una ciudad. Las nuevas tecnologías hacen accesible la recolección de información relevante sobre estas cuestiones, así como sobre las actividades de control, gestión y mantenimiento desarrolladas. La blockchain resulta muy adecuada para este tipo de registros por su capacidad para abarcar cuestiones diversas y generales, pero también tan concretas como la geolocalización, tipología y estado de salud de los árboles.

Más información sobre el impacto de la blockchain para las ciudades inteligentes en <libroblockchain.com/smart-cities/>.

Música, imágenes y un concepto más justo de la propiedad intelectual

Álex Preukschat

Desde el nacimiento del internet de la información, la libre distribución de contenidos digitales a un coste marginal cero ha supuesto una auténtica revolución, pues el coste adicional de comercializar o distribuir en este medio canciones, vídeos, imágenes o artículos periodísticos es prácticamente inexistente. Se ha generado así una explosión de la oferta que ha beneficiado a los usuarios finales de estos contenidos digitales, pero no a sus creadores, que si por un lado han visto que sus obras gozaban de una distribución global, por otro no han recibido compensación alguna desde un punto de vista económico por su trabajo. Se han visto, pues, abocados a una situación cada vez más precaria que les imposibilita vivir de sus creaciones, distribuidas o pirateadas sin control alguno.

Dentro del mundo de la blockchain hay dos movimientos vinculados que buscan redefinir la industria de los contenidos digitales. Por un lado, se encuentran las empresas que intentan crear nuevos protocolos descentralizados, como Mediachain.io o CoalaIP.org, para la etiquetación de contenidos digitales y su uso en bases de datos descentralizadas. Su apuesta es que, en el futuro, esas bases se conviertan en registros universales para licencias de contenidos digitales. Por otro lado, hay servicios y aplicaciones que lo que quieren es hacer uso de esos protocolos descentralizados para crear plataformas —centralizadas o descentralizadas— en las que los creadores de contenido tengan capacidad de etiquetar, almacenar, definir licencias o distribuir sus creaciones de forma descentralizada. Es un modo de que los artistas no pierdan el control sobre su obra y puedan en todo momento rastrear el uso dado a la misma y recibir una compensación monetaria por él.

El valor del rastreo de los contenidos digitales

Uno de los aspectos más innovadores del internet de la información es que en él todos podemos ser creadores y compartir nuestra obra con el mundo. Porque cuando publicamos un tweet o un artículo, o cuando compartimos una fotografía o un vídeo, estamos creando, y ello sin que nos guíe incentivo económico alguno. Por supuesto, no todo lo que creamos es interesante o relevante, pero el hecho es que nunca como hasta ahora había sido tan fácil llegar a tanta gente y compartir nuestras creaciones, un acto este que puede ser desinteresado, pero que repercute también en nuestra reputación y satisfacción personal. Porque el hecho de compartir (sea en el ciberespacio o fuera de él), lo mismo que el de ayudar a otras personas, contribuye a nuestra identidad y revela cómo queremos ser y cómo queremos que nos vea el mundo. Si tuviéramos protocolos descentralizados abiertos como los que ofrece la blockchain, asociados a licencias más flexibles, facilitaríamos la búsqueda, etiquetado y análisis de uso de contenidos digitales, y se podrían crear otros servicios de valor para mejorar el proceso de descubrimiento de creaciones digitales.

Cuando alguien comparte el tweet de otra cuenta, es posible notificar al creador original la existencia del retweet, y algo similar pasa en el resto de redes sociales. Con la blockchain sería posible tener un sistema totalmente abierto de notificación y rastreo universal para contenidos digitales, sistema que se podría automatizar porque todos los datos estarían en una plataforma común descentralizada. De este modo, el autor recibiría algún tipo de notificación siempre que se hiciera uso de una de sus obras y podría así ponerse en contacto con nuevas audiencias. Éstas, por su parte, podrían descubrir más creaciones del mismo autor. Y, por qué no, podría incluso existir una recompensa cada vez que se comparta una obra.

La monetización descentralizada para los creadores de contenido

Empresas como Monegraph, especializada en la monetización de contenidos digitales; Verisart o Ascribe.io, que lo está en el registro online de obras de arte, o Blockai, dedicada al registro de imágenes, están trabajando en la actualidad en aplicaciones y servicios que utilizan protocolos descentralizados de etiquetación y hashing basados en la blockchain. Es un primer paso para empezar a explorar una economía de nicho global descentralizada e inaugurar un nuevo escenario

dentro de los contenidos digitales en el que se pudiera reclamar derechos de autor de forma más eficiente. Las creaciones quedarían registradas en una blockchain construida al efecto y en la que los creadores podrían establecer sus propias reglas y precios gracias a contratos inteligentes. Por ejemplo, qué canciones son gratuitas, qué canciones son sólo para streaming, con qué calidad se pueden utilizar y el coste por el servicio solicitado. Ese registro sería público y cualquier persona o máquina podría leer las reglas de uso de los activos digitales inscritos.

Una máquina podría consultar las reglas programadas en un activo digital y crear servicios encima del registro de forma automatizada, prescindiendo de las infinitas negociaciones que suelen estar presentes en las condiciones de uso. Por ejemplo, la primera novela gráfica del mundo sobre Bitcoin (*Bitcoin: La caza de Satoshi Nakamoto*),[75] de la cual soy uno de los autores, podría con un sistema así vender partes de su contenido con contratos inteligentes para el uso en otras webs o publicaciones, y ello sin tener que pedir autorización. Los pagos por el uso de la propiedad intelectual se realizan de forma automática entre máquinas, lo que facilita también la vida a creadores y usuarios.

En este sentido, la compositora y violonchelista canadiense Zoe Keating[76] explica que, con el etiquetado y uso de metadatos abiertos de derechos de autor, se puede definir sin ningún género de duda a quién hay que pagar. Y eso es algo importante tanto para el creador como para el usuario, pues aunque parezca increíble puede llegar a ser muy difícil averiguar quién es el propietario legítimo de los derechos de una canción, a lo que se añade lo frustrante que resulta gestionar la compra de una licencia. En cambio, si contáramos con un libro mayor de metadatos de música sería muy sencillo localizar no sólo al creador, sino también a los músicos que intervienen, sus promotores. Y todo con la seguridad de que la información está actualizada. Con una plataforma así la actual industria de la música se vería radicalmente transformada, y para bien.

La correcta gestión de toda esta información serviría para crear una infinidad de nuevas aplicaciones basadas en el uso y las relaciones establecidas entre las partes involucradas. Por ejemplo, sería posible tener casas de intercambio en las que cotizaría el valor de activos digitales en tiempo real, con micropagos y dividendos para los colaboradores e inversores. El resultado sería

una nueva industria basada en los posibles ingresos futuros de los creadores, que recibirían así un apoyo directo y podrían prescindir de los intermediarios que tanto peso tienen hoy en la escena musical.

Imogen Heap,[77] por ejemplo, es una artista que ha conseguido desde el inicio de su carrera salir adelante sin necesidad de contar con la industria discográfica, a la que considera desfasada, fuera de la era digital, un desastre caracterizado por una contabilidad anticuada, contratos ininteligibles, retrasos en los pagos y errores en el etiquetado de la música. De ahí que defienda la desaparición, por innecesarios, de los intermediarios, una figura que, paradójicamente, es más numerosa en la industria que la de los propios artistas. Para Heap, el futuro de la música descentralizada podría gestionarse perfectamente a través de un proyecto conceptual al que denomina Mycelia.[78] Su ejemplo, como el de Zoe Keating, señala que la reestructuración del sector musical permitiría a los artistas vivir de su obra al darles el control de su distribución descentralizada y los beneficios económicos de todos los usos derivados de la misma. La discusión sobre la piratería de la música, que tanto perjudica a la cuenta de resultados de las discográficas, quedaría así superada, obsoleta. Todo el sector se reinventaría desde esos nichos de mercado.

Las economía de las aplicaciones blockchains descentralizadas

A pesar de todas las posibilidades que brinda la tecnología blockchain, lo cierto es que no es fácil aventurar cómo podría ser el proceso de transformación de la industria de los contenidos digitales. La estructura de cualquiera de los servicios o aplicaciones basados en la blockchain del futuro[79] podría tener tres capas.[80] La primera de ellas es la capa blockchain (una blockchain como Bitcoin o Ethereum, o las que sean relevantes en el futuro), que sería la encargada de gestionar el procesamiento de los contenidos digitales. La segunda estaría especializada en el etiquetado (un protocolo como Coala IP o Mediachain, por ejemplo) y sería la que gestionara los metadatos de los contenidos de forma descentralizada. La tercera y última capa es la de almacenamiento, que podría ser un servicio como IPFS (InterPlanetary File System) en combinación con IPDB (InterPlanetary Database). Todos los contenidos digitales quedarían almacenados de forma descentralizada y compatible con otras bases de datos.

El reto para los emprendedores en este campo es que no todo lo que es posible técnicamente es también legal. Un buen ejemplo de ello es el anuncio de Mediachain[81] de su buscador de imágenes universal, que recurre a bases de datos públicas de imágenes para su etiquetado, pero sin garantizar la propiedad intelectual de las mismas. La consecuencia de ello es que, si bien el proveedor de tecnología no incumple ninguna ley, el usuario final de esa imagen (por ejemplo, una web) sí puede ser denunciado por el uso ilícito que de ella haga.

En definitiva, y aunque es el mundo de la música[82] el que más interés está suscitando en el ámbito de la propiedad intelectual, hoy hay todo tipo de proyectos, y aún nacerán muchos más que querrán convertirse en plataformas descentralizadas universales[83] para todo tipo de contenidos digitales.

Más información sobre el impacto de la blockchain en la propiedad intelectual digital en <libroblockchain.com/propiedad-intelectual/>.

La descentralización de internet y la identidad digital

Álex Preukschat

Aunque el internet de la información nació como un sistema descentralizado, con el paso del tiempo se ha ido centralizando cada vez más. Los responsables de ello han sido empresas como Google, Facebook o Amazon, que, a la vez que desincentivaban la innovación, han ido concentrando a desarrolladores y usuarios en sus plataformas. Y, lo más importante, también una gran cantidad de información sobre nosotros. Ahí radica precisamente el efecto más evidente, por pernicioso, de la centralización experimentada por internet: que propicia que las grandes empresas del sector logren sus beneficios comercializando con la información del conjunto de sus usuarios. Así, cada vez que un hacker consigue robar información de un sistema centralizado surge siempre la misma pregunta: ¿no hay mejores maneras de gestionar la información de los usuarios de la red?

Como explica el profesor estadounidense Tim Wu en su libro *The Master Switch*, la tendencia natural de la evolución humana es pasar de etapas de descentralización a otras de centralización, y viceversa. Este internet más centralizado podría estar llegando a un punto de inflexión que abriría las puertas a un nuevo ciclo de descentralización. Estaríamos, pues, ante un cambio de ciclo que podría revertir algunas de las tendencias actuales y posibilitar, de nuevo, una innovación libre y sin restricciones. En este nuevo escenario, los desarrolladores trabajarán sin depender de las grandes plataformas y podrán desarrollar las soluciones que más les seduzcan, sin la obligación de ceñirse a las barreras de entrada que limitan actualmente a internet.

Esta nueva forma de trabajar y experimentar tendrá también repercusiones en los usuarios, menos dependientes de un software concreto para encontrar la oferta buscada. Y no sólo eso, sino que la gestión de la información, de forma individual y sin necesidad de estar centralizada en grandes empresas, será también más segura: al comprobar que no tendrán acceso a grandes depósitos de datos, los potenciales ladrones se verán desalentados.

Ahora bien, aunque las ventajas potenciales de la descentralización de internet son evidentes, hay que reconocer que crear estas soluciones descentralizadas es un reto técnicamente muy complejo.

El internet de la información centralizado actual

El modelo actual de internet ha derivado hacia la centralización de algunos de los componentes más importantes que imperan en su funcionamiento, como el sistema DNS (que redirecciona a los servidores con el contenido correspondiente), el sistema de certificación de seguridad de webs (ese candado verde que vemos en las páginas seguras HTTPS) o los sistemas de autenticación.

Cuando cualquiera de nosotros accede a una página web, ésta se localiza con un sistema que se llama DNS (Domain Name System) que convierte en un nombre fácilmente recordable por el usuario una dirección IP. Así, por ejemplo, <http://www.facebook.com> renombra una dirección IP 69.63.176.13 y facilita a los servidores el contenido que tienen que presentar al usuario. Este sistema de DNS, gestionado por ICANN (responsable de asignar las direcciones del protocolo IP), está relativamente bien descentralizado. Sin embargo, no es inmune a sufrir fallos de seguridad: es lo que pasó el 21 de octubre de 2016, cuando, en un ataque de denegación de servicio (DDoS, en sus siglas en inglés) contra la empresa Dyn (uno de los grandes proveedores de DNS), una gran cantidad de tráfico basura fue lanzado contra sus servidores. Durante horas, fue imposible en algunas zonas de Estados Unidos el acceso a páginas como Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast o la red de Playstation. Incluso compañías como GitHub,[84] un popular servicio para gestionar software de proyectos de código abierto, han sido irónicamente víctimas de ataques DDoS.

En lo que se refiere a los certificados que hacen seguras nuestras webs HTTPS, son emitidos por unas pocas empresas, muy grandes, como Verisign. Esta infraestructura de clave pública (PKI o *Public Key Infrastructure*, en inglés, que explicamos en más detalle en nuestra sección de criptografía) permite que las páginas webs que visitamos tengan el candado verde que garantiza tanto su seguridad como que estamos visitando la página que queremos visitar. Aun así, ha habido circunstancias exógenas a este procedimiento, como cuando el Gobierno turco[85] reemplazó —supuestamente por error— los certificados de

Google para servicios como Google Plus (una red social) y GMail (un servicio de correo electrónico), un ejemplo este de los abusos que un sistema centralizado de certificación puede sufrir desde el poder y que, en otro descentralizado, no serían posibles.

El último componente importante de internet lo constituye la identificación y autenticación de usuarios. Muchas personas identifican internet con servicios como Facebook o Google, y acceden a muchos otros servicios utilizando el mismo usuario y contraseñas que tienen en estas grandes empresas. De este modo, la red se convierte en una gran plataforma controlada por unos pocos grupos, pues éstos también están presentes incluso cuando accedemos a servicios ofertados por competidores distintos. Algunos hackers han demostrado que simplemente investigando a personas en redes sociales[86] e internet pueden averiguar información personal y tomar el control de sus identidades digitales sin necesidad de hackear técnicamente las cuentas personales de los usuarios. A eso se suman los robos de información a grandes empresas de todo el mundo. Es éste un evidente punto débil del actual internet porque la limitación por los problemas de seguridad dificulta el triunfo de la innovación.

El internet descentralizado de un futuro basado en la blockchain

En un internet descentralizado, también la identidad digital se verá descentralizada en los nodos participantes, lo mismo que la autenticación y los datos a los que accedemos. El resultado será un internet muy difícil de censurar y en el que no habrá puntos centrales de error o fallo. Y todo ello a un coste mínimo y garantizado por la propia inmutabilidad de la tecnología blockchain.

En la actualidad, el proyecto de protocolo descentralizado de código abierto más conocido y ambicioso es Blockstack, creado por Muneeb Ali y Ryan Shea. Junto a él, se puede citar también IPFS (Inter Planetary File System),[87] que trabaja en un protocolo de almacenamiento descentralizado. Su objetivo es reemplazar el protocolo HTTP por un internet con un funcionamiento similar a BitTorrent. Permacoin o Storj están también experimentando en la misma senda que IPFS.

Blockstack incorpora un software llamado VirtualChain,[88] que puede operar encima de cualquier blockchain pública como Bitcoin o Ethereum —o cualquier otra que pudiera hacerse popular en el futuro— y logra un nivel de seguridad sólo posible en un internet descentralizado. De este modo, Blockstack puede llegar a ser el instrumento que haga posible un internet descentralizado que no dependa de servidores (*serverless*, en inglés) y en el que los usuarios almacenen los datos en su propia nube. Se trata, en suma, de un gigantesco proyecto de código abierto en el que el sistema de DNS, la seguridad, la autenticación, la identidad y los pagos pueden actuar de forma descentralizada a través de una blockchain pública asentada como capa de referencia segura e inalterable.

En principio, el diseño de Blockstack no permite que un internet descentralizado basado en la blockchain de Bitcoin sea compatible con el internet descentralizado de otra blockchain pública, como Ethereum. Lo que les separa es el sistema de DNS de ICANN, pues Blockstack tiene un nuevo sistema de DNS basado en una blockchain con dominios .id (werner.id[89] es un ejemplo). No obstante, es posible que todos estos sistemas sean compatibles en el futuro. Navegadores como Chrome, Firefox o Safari, en cambio, sí podrían hacer posible el acceso a la red de Blockstack sin que los usuarios finales ni siquiera noten que han accedido a una infraestructura diferente de internet.

Usos y aplicaciones del internet descentralizado que propone Blockstack

En el internet del valor se podrán crear aplicaciones descentralizadas sin servidores, los usuarios almacenarán la información en su propia nube y la gestión de la identidad y los pagos estarán integrados de forma nativa en el protocolo. Si las soluciones de un internet descentralizado como Blockstack se hicieran populares en las tiendas de comercio electrónico,[90] podrían llegar a ofrecer soluciones de login, envío y pago con un clic e incluso competir con los grandes del e-commerce. Otro de los objetivos de Blockstack es permitir a los desarrolladores crear sistemas de correo electrónico resistentes al spam gracias a su sistema descentralizado.

En el internet descentralizado podremos establecer diferentes identidades digitales directamente en nuestro navegador y recurrir a ellas según el uso que

queramos darle a nuestra actividad en la red. De ese modo quedaremos identificados con la identidad que queramos en cada momento y no tendremos que acceder con otras claves a otros servicios. Los pagos que pudiéramos realizar podrán utilizar unidades de cuenta como bitcoin u otras criptomonedas.

Más información sobre el impacto de la blockchain para internet en <libroblockchain.com/internet/>.

La oportunidad del comercio electrónico

Adolfo Contreras Ruiz de Alda y Félix Moreno de la Cova

El e-commerce ha transformado por completo nuestra manera de comprar. Con un valor de mercado de cerca de dos billones de dólares,[91] constituye una industria que sigue creciendo a ritmos de doble dígito. Sin embargo, la falta de confianza en el modelo está interfiriendo en su pleno desarrollo.

En la actualidad, empresas como Amazon (en Estados Unidos y Europa) y Alibaba (en China) copan el comercio electrónico. Dado el enorme surtido de productos que ofrecen estas multinacionales, se han convertido en sitios webs de referencia, en la primera opción a la hora de buscar algo que comprar. Ése es el origen del círculo virtuoso logrado por estas empresas: el tráfico que generan es de tal calibre, que favorece también las ventas de las tiendas online afiliadas (*resellers*). Y, a la vez, esa dinámica tan favorable les proporciona el combustible necesario para mantener las visitas a Amazon o Alibaba en un índice muy alto. Amazon, además, permite una experiencia de compra homogénea, independientemente del producto que se compre. Es decir, un consumidor sabe lo que puede esperar en términos de calidad del producto, política de devoluciones, servicio de atención al cliente, precio o entrega, un patrón este que genera confianza e impulsa a los clientes a volver.

Esta centralización y acumulación de poder implica que Amazon es capaz de añadir comisiones de distribución medias del 15 % a los artículos vendidos. Si el trato entre fabricante y consumidor fuera directo, y no a través de un intermediario como es el caso, la supresión de estas comisiones supondría ahorros multimillonarios. No obstante, el comercio electrónico actual no está aprovechando la oportunidad que internet brinda de eliminar intermediarios, al contrario. La prueba es el desorbitado poder que está acumulando Amazon, que le permite prescribir la venta de productos de todo tipo, lo que a su vez frena el desarrollo de empresas, productos y negocios que sencillamente no cumplen los «filtros» impuestos por la compañía. Se trata de ventas que algunas empresas no pueden llegar a materializar y de productos que los consumidores no tendremos

oportunidad de descubrir nunca si no cuentan con el beneplácito de Amazon. Ésta, y lo mismo puede decirse de Alibaba en China, marcan en definitiva las reglas del juego.

Primer problema del comercio electrónico: los intermediarios y la generación de confianza

Para entender el futuro del comercio electrónico antes hay que conocer los problemas a los que se enfrenta en la actualidad y el papel que en ellos podría jugar la blockchain. Uno de los más importantes es el ya mencionado de los intermediarios.

En poco más de veinte años, la industria del e-commerce se ha convertido en un monstruo que va ganando en complejidad cada día que pasa. Y eso que el procedimiento para crear una tienda online es algo de lo más sencillo: bastan algunos clics. Además, es gratuito. La consecuencia es que hay millones de tiendas online en el mundo, aunque se estima que sólo 100.000 de ellas tienen ventas superiores al medio millón de euros anuales. También es digno de mención el tirón que han experimentado las empresas de mensajería de e-commerce, cuya facturación ha alcanzado ya los 20.000 millones de euros.

Tenemos, pues, a los principales actores en este sector: las tiendas online y las empresas de transporte, a las que se añaden los proveedores de tecnología y marketing online, además de todo tipo de intermediarios, tanto comerciales (*marketplaces*), como financieros (pasarelas de pago, emisores de tarjetas, bancos…). Una figura reciente es la del integrador de transportes, que permite a estas tiendas virtuales proporcionar a sus clientes una experiencia online homogénea en lo que se refiere a la navegación en el portal, el pago y la entrega de las mercancías. Se trata de un elemento importante, pues una experiencia homogénea es igual a mayor confianza, lo que a su vez significa mayores ventas.

Las tiendas pueden optar por vender directamente en su tienda o integrar su catálogo de productos en un marketplace, como puede ser Amazon. Cuando estos marketplaces son suficientemente grandes tienen sus propias pasarelas de pago. Es el caso de Amazon y Alibaba.

¿Por qué vender en Amazon?

Si eres una pequeña fábrica de juguetes de Pontevedra y deseas darte a conocer fuera de tu mercado natural, una buena opción es comerciar tus productos en Amazon. Es cierto que tu tienda online puede ser visitada desde cualquier punto del mundo, pero no lo es menos que difícilmente alguien de Nueva Zelanda ejecutará una compra en ella. Y no por antipatía hacia Pontevedra o porque el diseño de la web sea más o menos logrado, sino por una mera cuestión de confianza. Sencillamente, en las antípodas no te conocen.

En cambio, si comercializas esos mismos juguetes en Amazon, cualquier neozelandés que vea tu producto y le guste puede sentirse tentado a comprarlo por la sencilla razón de que está familiarizado con Amazon y conoce sus condiciones de venta. Eso sí, por esta intermediación que Amazon te brinda para dar confianza a tu producto, la compañía se llevará una importante comisión. A ella hay que sumar la que cobran otros intermediarios, los financieros, cuyo porcentaje gira en torno al 2% y 3 % del importe de la compra efectuada. Estos intermediarios financieros son las propias pasarelas de pago, así como los bancos con los que trabajan comerciante y cliente, y las entidades emisoras de las tarjetas con las que se efectúa el pago. Cada vez que se paga online, todos ellos se quedan con un trocito del pastel. Lo que una pasarela de pagos hace es recibir de manera encriptada los datos de la tarjeta del cliente, que acto seguido envía al banco del vendedor, que a su vez los reenvía al banco del cliente. Éste comprueba si la tarjeta cuyos datos ha recibido puede efectuar la transacción y, si todo está en orden, da su aprobación a la pasarela de pagos a través del banco del vendedor. Todo este proceso no tarda más que unos pocos segundos. Lo mismo ocurre si la pasarela de pagos es PayPal, Apple Pay o alguna empresa similar. En todos los casos se trata de servicios que tratan de aumentar la facilidad de uso del comercio electrónico, pero que, lógicamente, se llevan una comisión por el trabajo realizado, por lo general un 3 %. Aunque un 3 % de comisión pueda no parecer mucho, en un mercado de e-commerce mundial de casi dos billones de dólares representa aproximadamente 60.000 millones de dólares. Esto es, una gigantesca cantidad de dinero que si las tiendas no tuviesen que destinarla a esos intermediarios, podrían repercutirla en los precios de sus productos. Los beneficiados serían los clientes y no menos las propias tiendas, que podrían generar mayor demanda y ventas.

El e-commerce descentralizado del futuro

Existen varias iniciativas que persiguen un comercio electrónico en el que los intermediarios sean limitados, y en el que tanto compradores como vendedores puedan tener confianza en su contraparte. Aquí es donde entra en juego la blockchain. Un ejemplo de las nuevas posibilidades que brinda esta tecnología es OpenBazaar,[92] un protocolo de e-commerce descentralizado que funciona sobre un protocolo de Bitcoin, aunque también podría ser usado sobre otros protocolos de las blockchains públicas.

Creado por unos emprendedores estadounidenses, OpenBazaar es una ventana al futuro que muestra cómo podría funcionar el e-commerce descentralizado. Se trata de un software que todos los compradores y vendedores se instalan en su ordenador, sincronizando sus comunicaciones entre sí. Las transacciones son enviadas directamente a una cuenta *escrow* que sólo hace efectiva la operación una vez que el comprador confirme la recepción correcta del pedido. Esta cuenta *escrow* es como una cuenta puente en la que el dinero del cliente entra, pero no sale hasta que él mismo confirma la recepción del pedido en perfectas condiciones. En caso de disputas, y sólo en este caso, surge la figura de un «mediador», es decir, una persona que, por un módico precio, se ofrece a mediar hasta alcanzar una solución y que, mientras tanto, tiene el control sobre la cuenta *escrow*. Si en el e-commerce centralizado actual los intermediarios surgen en todas las transacciones, en OpenBazaar lo hacen exclusivamente en caso de disputas, lo que abarata considerablemente el funcionamiento.

OpenBazaar fue lanzado oficialmente en abril de 2016 tras un período de pruebas. Desde entonces decenas de miles de personas se han descargado ya en sus ordenadores este software que permite comprar y vender online sin intermediarios, y se han creado en su espacio miles de tiendas en las que las transacciones se realizan todavía en bitcoins. Pero lo realmente importante de OpenBazaar no es tanto esto como el desarrollo de protocolos sobre las blockchains públicas como la de Bitcoin, lo que abre una vía que puede constituirse en alternativa a Amazon y otros grandes operadores.

En definitiva, el objetivo de OpenBazaar es crear un entorno en el que impere la confianza (que es el auténtico motor del comercio) y prescinda de intermediarios que impongan sus precios y sus reglas. Que se trata de una proyecto atractivo y que va en serio lo demuestra el que varios inversores de

prestigio, entre ellos Union Square Ventures y Andreessen Horowitz, hayan invertido un millón de dólares en 2015 y otros tres millones en 2016 para que la propuesta de reinventar el e-commerce con las blockchains públicas se haga realidad.

Blockstack, otro internet basado en la blockchain

Otra iniciativa digna de mención en el campo del comercio electrónico descentralizado en un internet igualmente descentralizado es Blockstack, ya analizada en la sección dedicada a internet de este mismo capítulo. Union Square Ventures y SV Angel están invirtiendo en ella, con una aportación de un millón y medio de dólares en 2015 y otra de cuatro millones en enero de 2017.

Una aplicación fascinante de esta iniciativa sería la de poder navegar por cualquier tienda electrónica desde tu propio navegador y permanentemente identificado, es decir, sin necesidad de contraseñas o logins, ni del engorro de rellenar datos absurdos por triplicado cada vez que se visita una web. El funcionamiento estaría basado en la criptografía y posibilitaría la navegación con identidades anónimas no vinculadas a nuestras identidades reales. De este modo podríamos entrar en cualquier tienda online y, dado que la tienda nos identificaría sin lugar a dudas, podríamos hacer el check-out de un carrito en segundos, así como pagar también en segundos con nuestra cartera de divisas digitales asociadas a nuestro perfil. Al igual que en OpenBazaar, las transacciones se podrían hacer a través de una cuenta *escrow*.

Segundo problema del comercio electrónico: la entrega

Independientemente del éxito de los desarrollos de OpenBazaar, Blockstack u otros sistemas que surjan en el futuro, existe un problema recurrente que se puede resolver desde ya implementando una solución con tecnología blockchain: la entrega.

Las empresas de mensajería han crecido mucho aprovechando el tirón del comercio electrónico. Pero cuando compramos online, rara vez somos conscientes del esfuerzo que supone conseguir que esa compra llegue a su destino en los plazos que se manejan en la actualidad. Estas empresas de transporte tienen un problema añadido, y es que los usuarios finales ven en el servicio de entrega una *commodity* sin valor añadido diferenciador, es decir, un

servicio en el que prácticamente es imposible diferenciarse. Tanto es así, que a los usuarios nos parece lógico pagar 3 o 4 euros (o en muchos casos incluso no pagar nada) por un servicio que en 24 horas traslada cientos de miles de paquetes de una punta de España a otra. O desde otro país europeo en 48 o 72 horas.

Las empresas de mensajería pueden y saben perfectamente diferenciarse con un servicio de calidad que asegure la entrega, pero se encuentran con un impedimento: pocos usuarios desean pagar un plus para financiar esta diferenciación. Es más, tan convencidos están de que la entrega se efectuará sin problema, que consideran que no vale la pena pagar unos cuantos euros más para garantizarla. Por lo tanto, y para ahorrarse unos euros, el cliente se la juega, pensando que «malo será» que no llegue su compra a tiempo. Y esto pasa, a veces no llega, lo que genera una enorme insatisfacción, que aún se ve incrementada por la gestión de la incidencia que se pone en marcha entonces. El proceso es el siguiente. Digamos que las empresas de mensajería entregan en dos tipos de destinos: por un lado, en domicilios y oficinas; por otro, en puntos de conveniencia. Por lo general, los consumidores prefieren recibir en su domicilio, y para ello sí que están dispuestos a pagar un euro más. En lo que se refiere a los puntos de conveniencia, son mucho más baratos porque permiten «consolidar», es decir, agrupar muchos envíos en un solo viaje.

Cuando los usuarios se encuentran con problemas de entrega suelen atribuirlos a dos motivos: bien la propia ausencia del domicilio en el momento en que el mensajero pasó, bien porque ese mensajero nunca llegó a pasar. Las empresas de transporte han tratado de aportar soluciones parciales a estos problemas con la creación de los puntos PUDO (terminales de recogida) y los mencionados puntos de conveniencia, y también habilitando localizaciones alternativas de entrega o recogida de mercancía (en caso de que el cliente no esté en casa) o generando servicios de entrega en franja horaria. Igualmente, algunos transportistas han intentado crear soluciones en las que una foto del lugar de entrega sirviese como prueba de que el mensajero había cumplido con su obligación. Pero ¿cómo fiarse de este dato? ¿Cómo sabemos que esta foto fue realmente tomada el día de la entrega? ¿Y si no es más que un pantallazo sacado de Google Street View?

Es aquí donde la blockchain puede mejorar la experiencia del usuario de e-commerce: las tiendas online podrían solicitar a sus empresas de mensajería que, a través de una blockchain creada para ello o la utilización de alguna ya existente, pública o privada, registrasen los movimientos de sus mensajeros vía GPS, así como las fotos de los puntos de entrega. Toda esta información sería registrada con fecha y hora, y no podría ser alterada de ninguna manera. Las tiendas podrían acceder a ella de manera automática para asegurarse de que la entrega ha sido efectivamente hecha y para, sólo en ese caso, pagar el importe que corresponda, pues con esta información en la blockchain los pagos se podrían hacer de tal manera que sólo fueran ejecutados cuando el paquete fuese efectivamente entregado y no antes.

Por este servicio extra de recopilación y registro de los datos de entrega, las empresas de transporte podrían cobrar un plus que compensaría los gastos extra que les generaría garantizar la totalidad de las entregas de sus pedidos. Esa garantía, sin embargo, redundaría en la fidelidad de los clientes a las tiendas online, lo que a su vez haría que las empresas de transporte pudiesen financiar de manera justa un sistema de entregas más eficiente.

Todo esto no debe hacernos olvidar que la circunstancia de que un mensajero no se pase por un domicilio es un hecho consustancial a la estructura de las empresas de mensajería. Y seguirá siéndolo mientras no cambien los precios que esas empresas cobran en la actualidad, pues, por los motivos arriba descritos (el cliente quiere pagar poco), las operaciones de las empresas de transporte están diseñadas para ser capaces de entregar enormes volúmenes a precios muy bajos. Con esta estructura lo que hacen es crear rutas predeterminadas para cada mensajero, cada empresa con su método particular.

Estas rutas están hechas para entregar el mayor número de paquetes posible en el plazo prometido; repetimos, el mayor número de paquetes posible, ¡pero no todos! Por ejemplo, si la ruta y el horario de trabajo permiten a un mensajero entregar sesenta paquetes, pero llegan las fechas navideñas y se le pide que entregue ochenta, esos veinte paquetes de más no serán entregados. Si hay una segunda entrega, serán entregados al día siguiente, pero si son épocas de gran cantidad de envíos, volverá a pasar lo mismo, con lo que al final del segundo día serán cuarenta paquetes los que quedarán por entregar.

La insatisfacción que esto genera en los clientes se traslada no a la empresa de mensajería, sino a la tienda online, pues es a ésta a la que se ha pagado en el momento de realizar la compra. Un cliente insatisfecho por este motivo no suele volver, a lo que hay que añadir los comentarios negativos que pueda generar en las redes sociales. En esta situación, la tienda sufre un fuego cruzado entre la empresa de transporte y el consumidor. Es el momento de hacer juicios y actuar, pero no tiene elementos suficientes para optar por la decisión correcta. La blockchain, en combinación con otras tecnologías (como el uso de drones), podría ser una herramienta que mejorara sustancialmente la confianza entre todos los actores al efectuar las transacciones financieras sólo cuando haya pruebas digitales irrefutables de que las transacciones comerciales se han llevado a buen término para todas las partes.

El pago en el comercio electrónico con criptomonedas

En la actualidad existen más de setecientas criptomonedas,[93] de las cuales la única relevante para el comercio electrónico ha sido y es el bitcoin. Su uso para el pago de servicios y productos en el comercio electrónico fue una de las primeras ideas importantes que exploraron startups del ecosistema Bitcoin como BitPay. Ahora bien, las opiniones sobre por qué usar el bitcoin o cualquier otra criptomoneda como moneda de pago en este ámbito del e-commerce difieren. Por un lado, muchos de los primeros adeptos del protocolo Bitcoin siguen hoy viendo a la unidad de cuenta bitcoin, el token, como una moneda más: muchas veces los defensores más firmes de bitcoin como moneda son personas de Sudamérica que han tenido que sufrir en sus propias carnes todo tipo de experimentos monetarios de sus Gobiernos y bancos centrales. Por otro lado, Álex Preukschat y Javier Molina ya explican en su apartado de inversión en criptomonedas que antes de que bitcoin u otras criptomonedas puedan ser usados como dinero en el comercio electrónico tienen que crearse aplicaciones de uso reales que generen una demanda natural para las criptomonedas de estos protocolos. Es decir, se necesita un fundamento más sólido de demanda más allá de la mera especulación. Dicho esto, hay ventajas de las criptomonedas que ya están siendo utilizadas en el mundo del comercio electrónico, incluso como herramienta de marketing y ventas por empresas de viajes online como Destinia o Overstock.

El bitcoin, una forma de pago más

Como se explica en el capítulo dedicado a la banca, criptomonedas como el bitcoin permiten enviar dinero a nivel global y han sido uno de los factores que han animado a los principales actores del sistema financiero a invertir y mejorar sus servicios en diferentes ámbitos. La posibilidad de llegar a cualquier persona del mundo con capacidad de conectarse a internet sin necesidad de la existencia de una sucursal o espacio físico para la entrega del dinero ya se está utilizando para pagar servicios de personal técnico experto sin limitaciones. Posiblemente cuando el bitcoin (o cualquier otra criptomoneda) haya encontrado su nicho de mercado podría convertirse en algo así como el dinero de internet.

Aceptar pagos con bitcoins es tan simple como agregar una forma de pago más, junto con las habituales tarjetas de crédito y de débito, Stripe o PayPal. Para pagar con esta criptomoneda, en vez de introducir los datos de la tarjeta al uso, la web de compras muestra un código QR asociado a un dirección Bitcoin.[94] Seleccionada ésta, ya sólo hay que enviar a esa dirección el monto en bitcoins que muestre la web. Nuevas tecnologías como los protocolos NFC, ya integradas en muchos monederos bitcoin, están simplificando aún más los pagos y facilitando su uso.

En diciembre de 2016 eran más de 150.000 comercios a nivel mundial los que aceptaban pagos con bitcoins,[95] incluyendo pesos pesados como Amazon, Dell, Home Depot Expedia, Sears, Tesla o Zynga. BitPay es uno de los principales proveedores de pago con bitcoins del mundo. En agosto de 2015, el 60 % de los comercios que aceptaban bitcoins usaban BitPay,[96] un proveedor que ofrece la posibilidad de entregar el pago en bitcoins o convertir automáticamente el monto en moneda local. BitPay, además, ofrece integración a través de plugins con los principales proveedores de soluciones de comercio electrónico como Drupal, WordPress o Magento, así como instructivos «paso a paso» para programar desarrollos a medida. Eso sí, este tipo de servicio suele cobrar una comisión, por lo general el 1% de cada transacción.

Iniciativas para fomentar el uso de bitcoins

Muchos de los negocios físicos que dicen aceptar bitcoins (muchos de ellos recogidos en <https://coinmap.org>) han dejado de hacerlo simplemente porque casi ningún usuario utiliza esta criptomoneda para comprar servicios. Salvo los más convencidos o pudientes, la mayor parte de las personas prefiere acumular sus bitcoins, tal como se explica en el capítulo de inversiones. Las economías de red de un comercio local implican que, para que sea útil un medio de pago, debe ser utilizado por un porcentaje significativo de sus clientes o de los clientes potenciales dentro de su área de captación.

Experiencias como Calle Bitcoin en Madrid o Bitcoinstad en Arnhem (Países Bajos) han mostrado lo fácil que resulta implantar el bitcoin como medio de pago y, a la vez, el poco interés por mantener esta práctica si no hay una masa crítica de clientes que la demanden. La primera de ellas, Calle Bitcoin, fue una iniciativa lanzada en 2014 por un grupo de voluntarios en la comercial calle Serrano de la capital española. Allí, una veintena de comercios decidieron de forma coordinada aceptar bitcoins, atraídos por las ventajas de esta forma de pago. Sin embargo, dos años después sólo media docena de los veinte comercios originales continuaban permitiendo el bitcoin como forma de pago. Igualmente, los medios más sencillos empleados por estos comerciantes pioneros, ejemplificados por los «monederos de papel» (simples fichas plastificadas mostrando un código QR), han perdurado más que otras integraciones más complejas que requieren de procesadores de pagos y la necesidad de un dispositivo como medio de cobro. La intervención de la Agencia Tributaria, cuya oficina de prevención del fraude envió una carta en 2015 a todos los negocios participantes en la iniciativa pidiendo información sobre su uso de bitcoins, terminó de enfriar el entusiasmo inicial. La facturación (de escasos miles de euros en total) no justificaba tampoco cualquier riesgo potencial relacionado con las lagunas legales y fiscales de la criptomoneda. No obstante, los promotores de la iniciativa, como Félix Moreno, defienden la validez del experimento y pronostican que, especialmente en zonas turísticas, la sencillez de la integración, su bajo coste y la independencia respecto a intermediarios auguran un gran porvenir al bitcoin. Sólo es necesario que la adopción del bitcoin alcance una masa crítica de usuarios que asegure a las empresas un porcentaje suficiente de sus clientes pagando en esa moneda.

Un ejemplo que puede apuntar en esta dirección es la decisión, en 2016, de la mayor cooperativa de taxis de Italia de aceptar bitcoins en todos sus trayectos.[97] Asimismo, especialistas en TPV para pequeños comercios han integrado el bitcoin en sus terminales de pago con el objetivo de desintermediar a sus actuales socios bancarios y financieros, que acaparan la mayor parte del margen en su negocio.[98] La oportunidad para empresas como Ingenico o Verifone, con redes de decenas de millones de puntos de pago, de recibir pagos directamente es enorme. Sin embargo, es prematura a falta de una demanda por parte del cliente final. Sencillamente, no hay aún suficientes personas que tengan ingresos en criptomonedas y deseen gastarlas directamente para justificar este modelo. Esto podría cambiar en el futuro si gigantes como Airbnb[99] o Uber,[100] que actualmente dicen estar estudiando incorporar pagos en bitcoins, deciden lanzar dicha opción. Ello supondría poner al alcance de millones de personas recibir ingresos en bitcoins, de lo cual resultaría la creación de un mercado, primero en internet y como última etapa en los comercios a pie de calle.

El comercio electrónico y el comercio local se están fusionando y mezclando a pasos agigantados a medida que los teléfonos móviles se convierten en el primer dispositivo de acceso a internet para la mayoría de las personas. Samsung y Apple ya se han lanzado a la carrera por convertir al teléfono móvil en la principal forma de pago, con los grandes bancos compitiendo[101] fuertemente por no quedarse fuera de esta imparable tendencia. Las restricciones cada vez más extendidas sobre los pagos en metálico muestran la voluntad de los Gobiernos de aprovechar y potenciar esta tendencia.

Más información sobre el impacto de la blockchain para el comercio electrónico en <libroblockchain.com/ecommerce/.

Capítulo 4

Aplicaciones transversales de la blockchain

Carlos Vivas Augier

La gran mayoría de aplicaciones de la blockchain está por diseñarse e incluso por imaginarse. Es cierto que en el mercado existen productos como las criptomonedas o que hay aplicaciones transversales como contratos inteligentes (Smart Contracts), la integridad de datos (*data management*) y aplicaciones descentralizadas (*decentralized applications* o Dapps), pero ello no quita que sea un terreno abierto a la innovación y a las sorpresas.

Una de las grandes promesas de la blockchain son los contratos inteligentes o Smart Contracts. Sin entrar en tecnicismos, un contrato inteligente es un acuerdo entre partes con la capacidad de autoejecutarse. Esto que cabe en una frase es en realidad algo complejo que requiere de muchos elementos en sintonía. Un código informático, como podría ser el equivalente al «¡Hola mundo!» con el que suele iniciarse un programador, sería el equivalente de un contrato inteligente que define que si mañana llueve tú ganas 10 euros, y si no, yo gano 10 euros. Sin la blockchain, seguramente usemos uno de los siguientes mecanismos para gestionar este acuerdo:

- Firmaríamos un documento vinculante ante un notario.
- Elegiríamos a una tercera persona y nos someteríamos a su dictamen.
- Confiaríamos en el otro.

Si la apuesta fuera por mucho más dinero, la opción 3 no parecería la mejor. La primera, en cambio, aunque algo engorrosa, te da tranquilidad de que tienes el derecho a cobrar. Y usamos la palabra «derecho» intencionadamente, porque yo puedo negarme a pagar. La deuda se asume legalmente. Sin embargo, si la inversión para lograr el cobro legal no compensa el gasto invertido, quizá desistas de ir por ese camino.

Esto nos deja con la segunda opción. Así que buscamos una tercera persona, acordamos su comisión, digamos de 1 euro cada uno, le entregamos 10 euros cada uno y fijamos hora y lugar para encontrarnos el día de mañana para entregar al ganador la cantidad acordada. Si bien ésta parece la opción más conveniente, ¿qué pasa si el tercero en cuestión no aparece? ¿Y si está compinchado con el otro o en el último momento quiere cobrar más por la intermediación? La blockchain, como tecnología, resuelve los puntos flacos de las opciones planteadas y mantiene —e incluso potencia— las fortalezas. En el caso de lo engorroso de tener que ir a un notario, con la blockchain no haría falta, pues la cadena de bloques servirá de registro público —idea que desarrollamos más adelante—, por lo que el notario, como garante o certificador de la existencia del acuerdo, pierde su sentido. Un contrato inteligente prescinde de esta figura sin alterar el éxito de la ecuación. Por último, en el tercer caso, el hecho de que la blockchain embebe las dos primeras opciones, elimina la necesidad de que tú tengas que confiar en mí para recibir tu parte, y viceversa.

La problemática de los seguros

Supongamos ahora un nuevo producto del sector financiero: el seguro de vuelo retrasado. ¿No resultaría interesante que si tu vuelo llega a destino con más de dos horas de retraso te devuelvan el dinero que pagaste? Todos hemos experimentado el dolor de cabeza de un vuelo retrasado y todo lo que conlleva, pero todavía no están extendidas soluciones que den satisfacción a este problema. Mas si hay un alto interés del mercado y un bajo riesgo, ¿cómo es que el sector de las aseguradoras no ha sacado ya este maravilloso producto? La respuesta quizá la encontremos en el margen de negocio: la batalla de precios de las líneas aéreas es tan feroz, que un leve incremento para incorporar este servicio (ten en cuenta que el agente de seguros, la labor comercial, la persona que realiza la validación, los costes transaccionales, las reclamaciones, los pagos y otros imponderables suponen gastos) puede hacer que una tarifa deje de ser competitiva. Además, en caso de optar por este tipo de seguro, lo más probable es que transcurran más de noventa días antes de que recibas la indemnización.

Pues bien, el proceso de este mismo producto en la blockchain, tanto en una cadena privada como pública, se vería tan simplificado que su margen sería bastante mayor. Te lo explicamos mediante un ejemplo: tras comprar tu billete

Madrid-Oslo por, pongamos, 42,90 euros, salta una ventana con un anuncio que dice «por sólo 5 euros, seguro de retrasos. Si tu vuelo llega más de dos horas tarde, recupera tu dinero antes de que salgas del aeropuerto». Haces entonces clic en «contratar seguro», introduces tus datos personales, los datos de dónde quieres recibir la devolución, pagas, recibes una notificación con la información y listo. El día de tu vuelo Madrid-Oslo, el avión llega a tiempo. Pero a tu regreso, aterriza con cuatro horas de retraso. Mientras estás cambiando reuniones y disculpándote con tu jefe, ves una notificación de hace dos horas que dice que en un máximo de tres días habrán depositado 42,90 euros en tu cuenta de banco (y con criptomonedas, el pago sería casi en tiempo real).

¿Qué ocurrió una vez contratado este seguro? Una vez confirmado el pago, la aplicación de la aseguradora ejecutó el contrato inteligente utilizando tus datos personales, los datos de dónde reembolsar el coste del billete en caso de ser indemnizado, la información sobre el vuelo proveniente de la web de compras y cualquier otra información relevante para la compañía, como la fecha de contratación. De forma autónoma, el contrato inteligente comparó el horario de llegada del vuelo con los horarios de llegada publicados por las webs oficiales de cada aeropuerto (origen y destino). Si en alguno de los trayectos el vuelo no ha llegado a tiempo, con un margen de dos horas ejecuta las cláusulas, realiza el reembolso y se autodestruye[102] o desactiva, si bien permanece intacto en la blockchain por si es necesario auditar en el futuro la información.

Contrato inteligente, ¿o mejor «agente inteligente»?

Aunque el término «contrato inteligente» es el popularmente aceptado, la palabra «contrato» es a veces criticada, pues limita este tipo de contratos inteligentes a un caso de uso concreto (lo que viene a ser un contrato en el sentido más tradicional del término). Expertos en el tema, como John Stark, prefieren por ello términos como «agente inteligente» o *software agent*. Sea como sea, el concepto de contrato inteligente es anterior a la blockchain,[103] si bien es en el marco de esta tecnología donde ha tomado toda su fuerza. Más formalmente hablando, un contrato inteligente es un código informático que actúa como un acuerdo vinculante entre dos o más partes cualesquiera, sin necesidad de un intermediario, y cuyas cláusulas se programan previamente

otorgándole la capacidad de autoejecutarse validando, así, el cumplimiento de las condiciones de las cláusulas. Dicho de otra forma, cualquier contrato inteligente debe ser totalmente digital, debe tener capacidad sobre activos digitales, debe poder validar el cumplimiento de las condiciones acordadas y debe ejecutarse de forma autónoma y automática.

Es importante separar dos ámbitos de un contrato inteligente: el tecnológico y el legal. Nosotros vamos a centrarnos aquí en el primero, el tecnológico, dejando el otro aspecto para la sección legal de este mismo libro.

La programación de un contrato inteligente

Los contratos inteligentes pueden aplicarse en las blockchains privadas o públicas. Monax (antes Eris) o Corda de R3 son algunas de las plataformas con las que es posible utilizar contratos inteligentes en entornos empresariales o privados, mientras que en el entorno público tenemos Ethereum, cuyo origen fue pensado en aplicaciones sobre la blockchain en el sentido más amplio. Y está también Bitcoin, al que se están agregando capas que amplían las funcionalidades de su cadena de bloques a fin de hacerlas aptas para utilizar contratos inteligentes. Por ejemplo, RootStock está trabajando en esta opción. Otro servicio es SmartContract, que permite crear contratos inteligentes sin necesidad de saber programarlos. Digamos que intenta ser el equivalente de WordPress —y sus plantillas para la confección de páginas webs— para los contratos inteligentes.

Otra blockchain pública en la cual es posible usar contratos inteligentes es NXT, con la salvedad de que no puedes programar lo que quieres, sino que debes usar las «plantillas» existentes. Un caso particular es Blockstream, con su tecnología Sidechains, que permite que distintas cadenas de bloques se comuniquen entre sí y ejecuten contratos inteligentes, entre otras aplicaciones. Las particularidades y capacidades de cada una de estas soluciones van más allá del objetivo de este apartado. Lo importante es que de forma bastante rápida se están creando soluciones que responden a distintas necesidades en las que aplicar contratos inteligentes.

El proceso asociado a un contrato inteligente no es complejo de describir. El primer paso es programar el contrato inteligente (*code*). El hecho de usar un lenguaje de programación implica codificar exactamente lo que las partes desean que el contrato haga. A mayor complejidad de las condiciones, menor es la capacidad del contrato para realizarlas (hasta que la tecnología madure). En el contrato inteligente leeremos código en forma de «si esto, entonces aquello». Una vez escrito el contrato, el segundo paso es publicarlo en la blockchain, bien en una privada o una pública (*deploy*). El contrato está encriptado por lo que publicarlo no implica que éste pueda ser leído por terceros, si bien hay temas de seguridad y privacidad que tener en cuenta. Una vez publicado y almacenado en la blockchain, el contrato puede ser ejecutado (*call*). Dado que está en la blockchain, el contrato es ejecutado por los nodos y es necesario que se llegue a un consenso sobre el resultado. Según lo definido en el contrato, puede ser necesario actualizar la cadena (si hay un pago en criptomonedas, por ejemplo).

Una parte fundamental del contrato es su capacidad para validar el cumplimiento de las condiciones. Los oráculos u *oracles* proveen de información externa a la que el contrato inteligente no puede acceder (*inbound oracles*) y actúan en representación suya para ejecutar acciones externas fuera de su alcance (*outbound oracle*). En el ejemplo del seguro de vuelo, un oráculo podría ser el encargado de acceder a los datos de llegada de los vuelos, y otro, el responsable de emitir la orden de reembolso si es necesario comunicarse con el sistema de pago interno de la aseguradora. No siempre es más eficiente usar oráculos externos (*partial on-chain*), porque pueden incorporarse al propio contrato inteligente (*total on-chain*). Aun así, es importante saber que existen y que son útiles en casos en los que la información es externa a la blockchain o requieren de un menor esfuerzo computacional. Oraclize es un servicio que permite utilizar Web API como fuentes de información externa.

El hecho es que hoy los casos de uso y el alcance de los contratos inteligentes están limitados, tanto por la tecnología como por la regulación, si bien esta situación cambiará con el tiempo. En la medida que la tecnología avance podremos pasar de casos simples, como pagar a cambio del derecho de uso de un contenido digital, a otros más complejos en los que los contratos inteligentes gestionen nuestras finanzas y patrimonios. Tecnologías como el internet de las cosas habilitarán la capacidad de los contratos inteligentes de

controlar objetos cotidianos como una máquina expendedora o un vehículo autoconducido, y de realizar acciones de nuestra vida diaria como la compra del supermercado. En este escenario, un contrato va más allá de lo que formalmente podemos entender como tal, de ahí el comentario anterior sobre el término «contrato» y sus críticos. Por supuesto, seguirán existiendo casos en los que la mediación humana sea necesaria, por lo que jueces, notarios y abogados no corren riesgo de perder sus puestos de trabajo. Eso sí, estos profesionales deberán actualizarse para incorporar la capacidad de entender el código de un contrato inteligente o incluso saber redactarlo. El programa formativo de una carrera de Derecho deberá en breve incorporar estas habilidades.

Un reto muy importante en este ámbito del contrato inteligente es el relativo a la financiación. En la blockchain existe un coste computacional asociado a inscribir cualquier cosa en la cadena de bloques. Cuanta mayor complejidad tengan los contratos inteligentes, mayor será el coste computacional asociado. Y no sólo en equipos informáticos, pues hay también otros costes asociados, como la energía empleada o el ancho de banda utilizado, por ejemplo. Modelos en los que el consenso es a través de nodos asignados (*federated*) o de mayor peso de la red (*Proof-of-Stake*) podrían ser soluciones que reduzcan el coste computacional. Los oráculos también podrían ayudar a mitigar el problema. Sin embargo, es un reto importante, ya que de su resolución depende que los contratos inteligentes lleguen a dar o no su mayor potencial.

Integridad de datos, un registro único y global

Moverse en un entorno descentralizado implica que todos los que lo integran toman o pueden tomar parte en lo que ocurre. Ello otorga atributos muy valiosos a los datos en la blockchain porque ninguna parte de forma individual puede escribir en la cadena de bloques. De la misma forma, los datos no pueden ser manipulados por ninguna de las partes de forma individual y siempre tendrán como atributos el momento de inscripción y su(s) autor(es). Por ello, cuando se habla de blockchain y datos siempre se usan palabras como transparencia, trazabilidad, integridad, autoría o registro, sin que ninguna parte, de forma individual, otorgue esas cualidades al conjunto. Esto implica que la veracidad de los datos no depende de la reputación, potestad y/o validez de un certificador, custodio o autoridad central.

Dicho lo anterior, es fácil entender el potencial de la blockchain como registro público de activos, no exclusivamente digitales, que permite definir la propiedad o titularidad, la trazabilidad y el uso de dichos activos. Supongamos que eres un aficionado de la bici de montaña y has comprado una Trek Slash 9.8 29 de 5.500 dólares. Dado su valor, quieres tener la capacidad de demostrar que es de tu propiedad en situaciones como un posible robo y posterior recuperación por parte de la policía. En un mundo sin blockchain, guardar la factura con los datos de la bicicleta en un lugar seguro no es una mala opción, pero aun así ese documento puede perderse, deteriorarse o que se ponga en duda su autenticidad si el comercio donde hiciste la compra cerrase. En cambio, en un mundo con blockchain podrían hacerse dos cosas. La primera, tomar una foto de la factura, generar un hash asociado la imagen y publicarlo en la base de datos de la cadena. El valor añadido de la blockchain, sobre meramente digitalizar la factura, es el registro del tiempo (*proof-of-existence* o *time-stamping*) y la titularidad de haber sido tú quien hizo ese registro. Pero en un mundo blockchain avanzado se podría hacer de una forma mucho mejor: el fabricante de la bicicleta registra el activo en la blockchain. Una vez éste vendió la bicicleta al comercio, el fabricante traspasa la propiedad del activo al comercio, y cuando tú compras la bicicleta, el comercio hace lo mismo contigo. Este proceso permite la trazabilidad completa del activo certificado, que no es ni una falsificación ni el fruto de un robo.

Ahora supongamos que has comprado la bicicleta para alquilarla a otros aficionados a la bici de montaña. No quieres ceder la propiedad del activo, pero tu cliente prefiere no correr el riesgo de que reportes la bici como robada mientras él la está usando. Pues bien, valiéndote de la blockchain y un contrato inteligente podrías ceder temporalmente el derecho a uso del activo durante el período que dure el alquiler. En este ejemplo suponemos, además de un mundo digitalizado (al cual nos dirigimos), que la blockchain está reconocida como registro público. Su carácter digital le otorga propiedades como la agilidad y accesibilidad de los datos. Hoy la tecnología ya permite gestionar propiedad, trazabilidad y uso de activos, pero su validez como registro requiere aún del reconocimiento legal por parte de las entidades jurídicas.

Dapps y DAO, hacia la descentralización

Se dice que una tecnología es «entre pares» (*peer-to-peer*, P2P) cuando en ella la desintermediación es la regla; es decir, cuando la continuidad y funcionalidad no dependen de una sola parte. No obstante, como suele suceder con muchos términos nuevos, la definición generalmente aceptada no es «única». David Johnston[104] define que una *decentralized application* (Dapps) es aquélla en la que:

- El código es abierto (*open-source*) y las mejoras son aprobadas en consenso con los usuarios de la aplicación.
- Los datos y registros están encriptados y almacenados en una blockchain pública y descentralizada.[105]
- Se necesita un token criptográfico (como el bitcoin) para acceder a ella y las contribuciones de valor de los mineros se recompensan con éste. Ninguna parte puede controlar la mayoría de tokens.
- Se generan tokens siguiendo un algoritmo criptográfico estándar como prueba del valor que los nodos añaden a la aplicación (*Proof-of-Work* de Bitcoin).

Más allá del concepto, la importancia de las Dapps es que constituyen un nuevo modelo de aplicaciones y el futuro de la web.[106] Bitcoin demostró que este nuevo modelo es técnicamente factible y económicamente viable. Las principales aplicaciones que usamos del internet de la información (Amazon, Airbnb, Dropbox, Facebook, Gmail, Uber o WhatsApp) funcionan bajo un modelo centralizado y muchas podrían funcionar de forma descentralizada. No es sorprendente que muchas de las primeras Dapps propongan alternativas a los gigantes del mundo digital, como OpenBazaar para eBay, Storj para Dropbox, La'Zooz para Uber y FireChat o Gems para WhatsApp, entre otras.

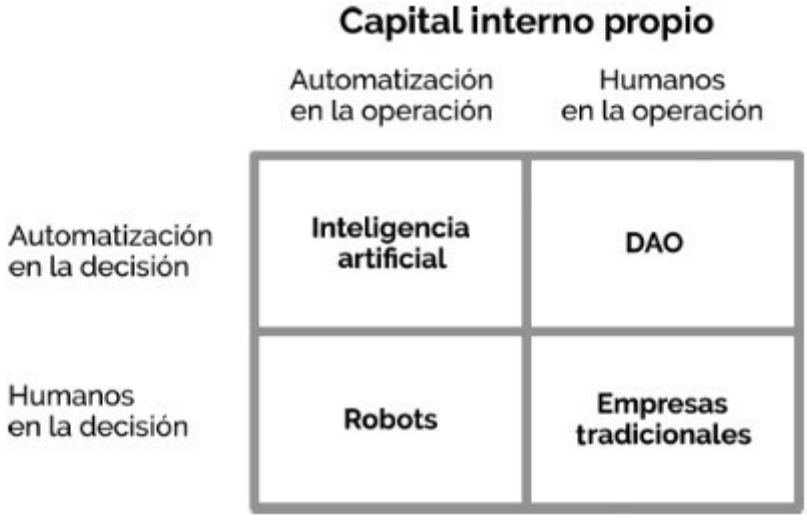
El pagar o no por estos servicios son opciones viables. La mayoría de usuarios de Facebook considera que es un servicio gratuito, pero no lo es, pues pagas con tu información personal, gracias a la cual la compañía ha hecho miles de millones de dólares. Los clientes de Facebook son las empresas que se anuncian en su plataforma. Usando Dapps se habilitarán nuevas opciones en las que aceptas compartir todos o parte de tus datos para acceder a los servicios, o incluso recibir ingresos por el uso de tus datos como recompensa a contribuir

con la Dapp. Sin ser la única alternativa, una de las plataformas más usadas es Ethereum Blockchain. Desde el origen, su objetivo ha sido el de habilitar un entorno para desarrollar aplicaciones basadas en la tecnología blockchain. State of the Dapps (<http://dapps.ethercasts.com>) es un buen repositorio para explorar casos de uso y conocer en qué está trabajando la comunidad de desarrolladores de Ethereum.

Las Decentralized Autonomous Organizations (DAO)

Las *Decentralized Autonomous Organizations* (DAO) vendrían a ser una subclase de Dapps. Antes, sin embargo, de ir más adelante conviene definir bien dos conceptos: *Decentralized Organizations* (DO) y *Automated or Autonomous Agents* (AA). El primero hace referencia a un modelo de organización en el que un conjunto de personas interactúa entre sí siguiendo un protocolo (esto es, las reglas y condiciones de funcionamiento) definido en código y ejecutado en la blockchain. De este modo, el «poder» se distribuye de forma más equitativa entre los participantes. Y estas personas no tienen por qué ser las únicas que tomen decisiones, sino que los contratos inteligentes pueden participar también en ellas. Por otro lado, los AA son el sueño de la inteligencia artificial, autómatas capaces de emular al cerebro humano (con las ventajas añadidas que otorga la tecnología) y tomar decisiones, adaptarse a las circunstancias, evolucionar y ser autónomos en su existencia. En la actualidad no existen versiones tan avanzadas de esto, pero sí sencillas, como los virus informáticos.

Esquema de decisión y operación para el uso de robots o humanos según el modelo de negocio.



Fuente: Elaboración propia en base a un esquema propuesto por Vitalik Buterin.

Las DAO vendrían a ser DO, sólo que las decisiones las toman AA, no seres humanos. Vitalik Buterin,[107] cofundador de Ethereum y Bitcoin Magazine, las define como entidades que «viven» en internet, existen de forma autónoma y dependen de personas para realizar aquellas tareas que no pueden ejecutar por sí mismas. Una característica importante es que las DAO tienen un capital interno de valor que sirve para remunerar, por ejemplo, el trabajo de sus empleados humanos.

Un tipo de DAO son las *Decentralized Autonomous Corporations* (DAC), cuya principal característica es que en ellas se pagan dividendos. Es decir, que integran el concepto de acciones como si se tratara de una empresa tradicional, con todo lo que ello implica en cuanto a beneficio y toma de decisión. De momento, los casos de uso son escasos. Bitcoin cumple con varios de sus requisitos, pero para muchos no es una DAO, ya que no es «lo suficientemente inteligente».

Más información sobre las aplicaciones transversales de la blockchain en <libroblockchain.com/contratos-inteligentes/>.

Capítulo 5

¿Cómo invertir en la blockchain?

Álex Preukschat y Javier Molina Jordá

La diferenciación entre las blockchains públicas y las blockchains privadas (también conocidas como Distributed Ledger Technology, DLT) se hace especialmente evidente cuando se trata de inversión. La razón no es otra que cada una de estas tecnologías tiene modelos de financiación e inversión completamente diferentes, si bien ambas se sustentan en los principios básicos que rigen la blockchain.

Las blockchains privadas están financiadas principalmente por consorcios de empresas —sobre todo del sector financiero y bancario— y con capital riesgo, aunque no son iniciativas exclusivas de un único sector. Algunos de los proyectos más conocidos de tecnología blockchain privada son R3, Chain, Digital Asset Holdings, Ripple o Hyperledger, a los que haremos referencia en la sección de tecnología blockchain privada de este libro. Son la punta de lanza de otros muchos proyectos que vendrán en el futuro. Ahora bien, lo realmente revolucionario en este sector no viene de la mano de esta categoría de las blockchains, sino de las públicas, y ello gracias al nacimiento de Bitcoin en 2009. A ellas vamos a dedicar estas páginas.

La economía de los protocolos basados en las criptomonedas

La blockchain pública se ha hecho famosa y ha logrado financiarse a través de la emisión de criptomonedas como bitcoin o ether, lo que la convierte en uno de los pilares fundamentales de lo que podría ser el internet del valor. Pero para entender en qué consiste esta nueva economía antes es necesario explicar el modelo de financiación creado en el ecosistema de las blockchains públicas. Se trata de un concepto tan original, que podría cambiar o destruir a algunas de las empresas establecidas y consolidadas del actual internet de la información.

El protocolo como fuente del internet del valor

La palabra «protocolo» aplicada a la tecnología suele evocar la idea de algo inverosímilmente complejo e ininteligible. Y aunque hay parte de verdad en eso, en el fondo un protocolo tecnológico no es más que un sistema de reglas que permiten que dos o más ordenadores se comuniquen entre sí para transmitir información. Durante años, fue un terreno cerrado, algo que comités de expertos de gobiernos y grandes empresas desarrollaban y que acababa siendo una fuente de interminables conflictos económico-empresariales. Todo esto cambió con la creación del protocolo Bitcoin, que democratizó la financiación y el desarrollo de protocolos abiertos, y abrió las puertas a un nuevo escenario descentralizado.

Uno de los protocolos descentralizados más famosos en el mundo actualmente es BitTorrent, un sistema descentralizado Peer-to-Peer (P2P o «entre pares» en castellano) que facilita el intercambio directo de contenidos (como películas o música) entre ordenadores sin la necesidad de contar con un ente central de confianza. iTunes de Apple o Netflix serían un ejemplo de lo mismo, pero en versión centralizada. Otra característica es que, para ser usado, BitTorrent no necesita de una criptomoneda o token asociado como incentivo en su sistema, pues el valor de poder compartir contenidos con otros usuarios ya es suficiente motivación para muchas personas que almacenan películas y canciones en sus ordenadores.

Lo que ha hecho Bitcoin es combinar la tecnología P2P con la criptografía de clave pública, lo que, junto con la estructura de incentivos de blockchains públicas de tokens (bitcoins, ethers, etc.), fomenta el mantenimiento, utilización y participación de protocolos abiertos. En definitiva, se trata de una revolución del hasta entonces aburrido mundo de los protocolos.

¿De qué sirve un token en un protocolo?

Para usar el protocolo Bitcoin se necesita un token, el bitcoin. El protocolo se llama Bitcoin con «B» mayúscula, mientras que la unidad de cuenta, el token, es bitcoin, con «b» minúscula. La unidad de cuenta bitcoin (moneda es *coin* en inglés) se denomina «criptomoneda» porque el objetivo del creador del protocolo Bitcoin, Satoshi Nakamoto, era el de crear un sistema de pagos descentralizado que estuviera gestionado por una comunidad sin la necesidad de un tercero de confianza centralizado. De ese modo podría prescindirse de

bancos comerciales o bancos centrales. Desde entonces, todos los protocolos descentralizados que se inspiraron en Bitcoin han llamado a sus unidades de cuenta «criptomonedas», a pesar de que el nombre más correcto es el de token.

En un protocolo descentralizado, un token toma forma como una cadena alfanumérica, tipo 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNL, y representa un identificador en la base de datos descentralizada de consenso, como es el caso de Bitcoin. Es algo que equivale, pues, a las anotaciones realizadas en cualquier otra base de datos centralizada, como la de nuestro banco, sólo que en este caso hablamos de una base de datos descentralizada que no está controlada por un ente central. Estos identificadores, además, se pueden compartir directamente entre personas y sin intermediarios a nivel P2P.

¿Qué sentido tiene invertir en criptomonedas o tokens de protocolos descentralizados?

La capitalización del mercado Bitcoin ha fluctuado en los últimos años entre 6.000 y 14.000 millones de dólares hasta 2016 (número de bitcoins emitidos, multiplicado por el precio de mercado). La segunda criptomoneda en el escalafón con más capitalización ha sido el ether de Ethereum. Sin embargo, estos listados cambian regularmente según el progreso tecnológico y las expectativas sobre las criptomonedas que se generen en el mercado.

Los inversores o especuladores convencidos compran estas y otras criptomonedas porque apuestan por el potencial futuro de estos sistemas descentralizados, así como por la posibilidad de que atraigan a innovadores que construyan soluciones y aplicaciones sobre estos protocolos públicos y abiertos. En caso de que triunfen, necesariamente habrá que utilizar tokens para operar en el protocolo y tener acceso a bases de datos descentralizadas o blockchains públicas.

Esta circunstancia ha posibilitado que una comunidad de inversores globales, afines a la tecnología, invierta en protocolos abiertos que históricamente no tenían un modelo de negocio directo. Por establecer una comparación, TCP/IP, HTTP o SMTP son algunos de los protocolos que han permitido crear el internet de la información tal y como hoy lo conocemos. Y han sido la base sobre la que se ha sustentado el éxito de empresas como

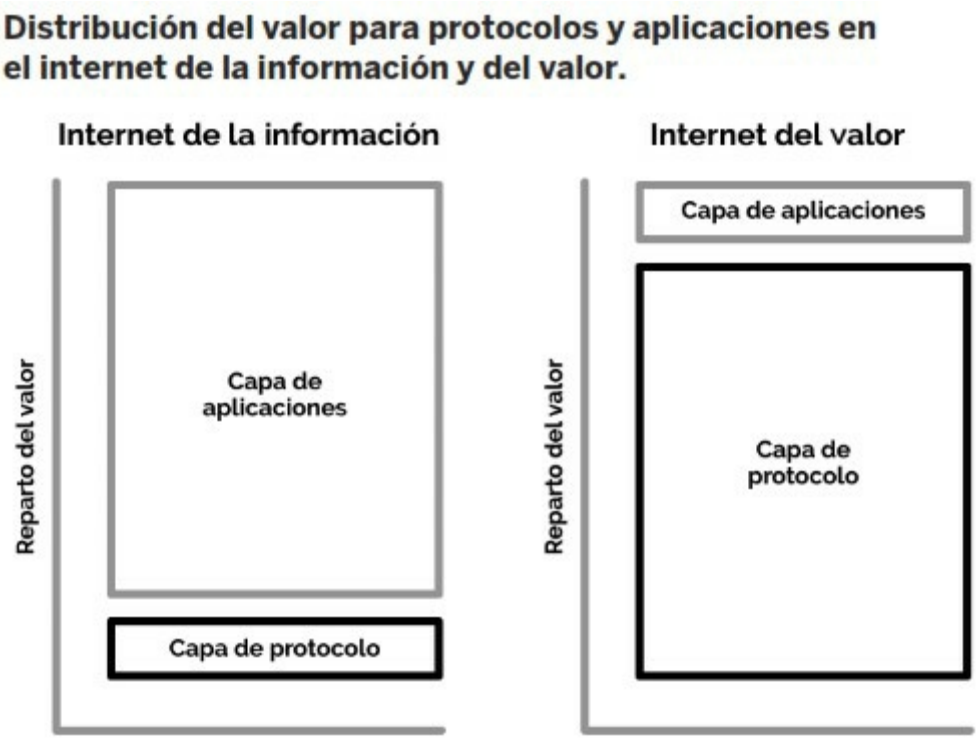
Amazon, Google o Facebook, entre otras muchas. Sin la existencia de estos protocolos previos y su correcta utilización, ninguna de las citadas empresas hubiera podido desarrollar su modelo de negocio.

La creación de los tokens de las blockchains públicas, como bitcoin o ether, imprescindibles para el uso de estas plataformas, ha posibilitado un mercado que incentiva la inversión en estos desarrollos y ha convertido en noticia y objeto de fuerte especulación el hasta entonces mundo gris de los protocolos desconocidos. El efecto positivo de esta revolución es que ha acelerado el ritmo de innovación, independientemente de intereses gubernamentales o empresariales. Así, en todo el mundo se puede apostar ya libremente por protocolos que podrían ser la base fundamental para crear el próximo salto de innovación tecnológica tras el internet de la información.

Pero todo esto tiene también su lado negativo: la expectativa generada en el mercado de las criptomonedas ha propiciado una gran cantidad de fraudes. Por lo tanto, lo natural es que muchos de los proyectos puestos en marcha fracasen. Con el tiempo, los más aplicables irán consolidándose y, con ello, asistiremos al nacimiento de los futuros líderes de las blockchains públicas y del internet del valor.

La economía de los protocolos descentralizados basados en tokens

La figura que se va a llevar el beneficio en esta nueva estructura económica descentralizada son los protocolos. Esta previsión toma forma en la expresión *Fat protocols* (protocolos gordos) *versus Thin apps* (capas de aplicaciones delgadas), que plasma lo que será la futura redistribución del valor desde la capa de aplicaciones propia del internet de la información a la capa de protocolos del internet del valor. Hasta ahora, los inversores han invertido en la capa de aplicaciones porque es ahí donde se concentra el valor, pero esto no tiene por qué ser así en el futuro.



Fuente: Joel Monegro/Union Square Ventures[108] con adaptaciones.

Aunque la palabra suele tener connotaciones negativas, lo cierto es que es la especulación lo que hace posible todo este ciclo virtuoso de innovación tecnológica y lo que proporciona liquidez al mercado. El protocolo Bitcoin, así como la mayoría de protocolos serios de éxito, opta por una emisión deflacionaria de las monedas, al crear un monto finito en el tiempo (en el caso de Bitcoin serán 21 millones de bitcoins creados hasta el año 2140) con el que recompensar a sus inversores iniciales. A mayor demanda y expectativas de futuro, los precios por tokens se revalorizan pudiendo llegar a compararse a una gran burbuja financiera. Así, el ciclo de especulación frenética y explosión de burbujas en el mundo de las criptomonedas y los protocolos descentralizados adquiere una consideración necesariamente positiva, porque fomenta una constante innovación.

Lo interesante es que las aplicaciones de éxito atraen nuevos usuarios al protocolo y eso hace que los inversores que ya tomaron posiciones en su momento las mantengan a la espera de revalorizaciones futuras de sus participaciones en forma de tokens o criptomonedas. De este modo, al reducirse la oferta de criptomonedas, aumenta su precio. La consecuencia de este incremento en la capitalización de mercado del protocolo (esto es, del número de criptomonedas emitidas por el precio de mercado por unidad) es una

atención generalizada que suele verse recompensada con nuevos inversores y desarrolladores. El efecto logrado, según USV, es la redistribución del valor en el internet del valor. Si se cumple esta previsión, la capitalización de un protocolo crecería más rápido que todas las aplicaciones juntas que hacen uso de ese mismo protocolo. ¿Por qué? Porque el éxito de las aplicaciones acelera la popularidad del protocolo y fomenta la competencia en la capa de aplicaciones, el valor de la cual podría acabar concentrándose en la capa de protocolo. Por tanto, estos protocolos se convertirían en acaparadores «gordos» del valor, mientras que las aplicaciones serían las «víctimas» de este hecho singular, al acaparar una parte menor del valor que la que han tenido históricamente por compartir todas una misma base hipercompetitiva y por competir sólo por la parte más pequeña del valor en el internet del valor.

De estas nuevas estructuras económicas nacerán las empresas basadas en protocolos que reharán el internet de la información, y ello a pesar del mayor peso que los protocolos abiertos tendrán en una nueva distribución del valor entre aplicaciones y protocolos. En este nuevo ecosistema, todos podremos invertir o especular desde el principio a diferencia de lo que ocurre en el internet de la información, que limita esta posibilidad a los grandes inversores institucionales hasta la salida a bolsa. Que USV y Andreessen Horowitz[109] comparten esta misma visión lo demuestra el que en 2016 hayan invertido 10 millones de dólares en un fondo especializado únicamente en criptomonedas. Por otra parte, USV ha sido de los más activos invirtiendo en protocolos que operan encima de Bitcoin o Ethereum con nuevas funcionalidades. Blockstack (tratado en el capítulo de internet e identidad digital), Mediachain (que explicamos en el capítulo dedicado a la propiedad intelectual) o OB1 de OpenBazaar (abordado en el capítulo de comercio electrónico) son sólo algunos ejemplos de esta tendencia.

¿Cómo se compra o invierte en criptomonedas?

Hay tres modos de adquirir criptomonedas. Del más sencillo al más complicado, son:

1. **Exchanges:** se trata de una casa de cambio en la que se pueden comprar y vender criptomonedas.

2. **Intercambiando bienes y servicios:** a cambio, se recibe un salario en criptomonedas.
3. **Minería:** minando bloques en una blockchain basada en prueba de trabajo (PoW).

Como se ha dicho, el modo más sencillo son las casas de cambio. Dentro de éstas hay que diferenciar entre aquellas en las que se pueden intercambiar bitcoins u otras criptomonedas por euros o dólares, y aquellas otras en las que la «moneda» de referencia es el bitcoin. En este último caso es necesario poseer ya bitcoins para poder intercambiarlos por las otras criptomonedas. Todas las casas de cambio serias operan con un procedimiento de identificación de clientes (conocido en inglés como Know Your Customer-KYC) que obliga a los nuevos usuarios a identificarse y cumplir con las disposiciones legales relativas a la prevención de blanqueo de capitales (el Antimoney Laundering-AML). Por otro lado, abrir una cuenta en un Exchange es lo más parecido a hacer lo propio en una entidad bancaria. De hecho, a veces puede resultar frustrante debido a los múltiples procesos administrativos impuestos para poder operar. El reto para estas casas de intercambio es sobrevivir a los muchos fraudes o robos perpetrados por hackers, que han provocado que sólo hayan sobrevivido las más eficaces, como Bitstamp.net, Kraken.com, Coinbase.com o Xapo.com. Sin embargo, tampoco tenemos garantías de que éstas sigan existiendo en el futuro, pues bien es posible que sufran un ataque que obligue a su cierre y liquidación. Suceda o no, las víctimas son siempre las empresas centralizadas y sus usuarios, pues desde 2009 ningún hacker ha conseguido atacar el protocolo Bitcoin a pesar del importante incentivo económico y el prestigio que lograría labrarse quien lo lograra.

En cuanto a la segunda opción, ya hay algunas empresas que pagan a sus empleados con criptomonedas. Es el caso de la empresa de seguridad online Cobalt.io, que utiliza bitcoins para remunerar a sus investigadores, independientemente del país en el que vivan. Igualmente, algunos profesionales liberales aceptan esta forma de pago por sus servicios.

La tercera opción es obtener bitcoins minando. El proceso de minar se realiza para criptomonedas que tienen un sistema de Prueba de Trabajo (Proof of Work, en inglés) que asegura las transacciones gracias a la capacidad de

cálculo de un ordenador o granja de ordenadores. En los últimos años, la minería de criptomonedas se ha profesionalizado tanto, que no suele ser rentable para una persona que no tenga la capacidad técnica y el capital necesario para realizar grandes inversiones. Es decir, que ganar dinero minando resulta complicado en las criptomonedas más populares.

Dos son los métodos de minería principales: la Prueba de Trabajo (Proof of Work), utilizada en el protocolo Bitcoin o Ethereum, y la Prueba de Participación (Proof of Stake), por la que los propietarios de criptomonedas son recompensados de forma progresiva con nuevas unidades del mismo tipo en una lotería entre los propios tenedores. Este modelo, a diferencia del primero, permite una distribución de criptomonedas basada en las prioridades de los desarrolladores del protocolo. Lamentablemente, ha facilitado la proliferación de muchos casos fraudulentos.

En el modelo de Proof of Stake se suele realizar una operación conocida como «preminado», por la que los desarrolladores del protocolo distribuyen una cantidad fija de criptomonedas a un grupo reducido de inversores y más tarde —abierta ya la distribución al público en general— intentan inflar los precios de esta nueva criptomoneda para obtener mayores beneficios, siempre que la campaña de marketing sea exitosa. Obviamente, esto no significa que todos los modelos de Proof of Stake sean fraudes, pero sí es verdad que los propician, a diferencia de lo que pasa en Proof of Work, en el que el desarrollador de un protocolo difícilmente puede controlar la distribución de las monedas.

El ICO en el mundo de las criptomonedas

En el mundo de las criptomonedas o criptodivisas se utiliza un instrumento que se conoce como Initial Coin Offering u Oferta Inicial de Moneda (ICO, de sus siglas en inglés) y sirve para financiar el desarrollo de nuevos protocolos. En el fondo, es como una salida a bolsa al uso, pero de un protocolo descentralizado y sin un régimen regulatorio y legal definido.

Algunos de los ICO más conocidos del mundo de las criptomonedas están vinculados al protocolo de Ethereum. Durante su campaña de lanzamiento en el verano de 2014, Ethereum recaudó 31.531 bitcoins (15 millones de dólares del momento) gracias a un sistema de preminado, si bien los inversores tuvieron

que esperar un año para poder negociar sus ethers en el mercado, porque así se estipulaba en el pacto de inversión del ICO adoptado para frenar la especulación inicial.

En su momento, este lanzamiento de ether fue una de las campañas de crowdfunding más exitosas registradas en cualquier protocolo y posicionó a Ethereum y su criptomoneda como un serio competidor que podría recibir atención de desarrolladores e inversores en el mercado de las criptomonedas, incluso en competencia con el protocolo Bitcoin. Desde entonces, algunos de los ICO más sonados e importantes de nuevos protocolos descentralizados han utilizado Ethereum como protocolo de referencia. A continuación explicamos algunos de ellos.

El ICO de TheDAO

El ecosistema de Ethereum hizo de nuevo historia en 2016. El 30 de abril de ese año, la startup del ecosistema Ethereum Slock.it anunció el lanzamiento de TheDAO a través de una campaña de financiación colectiva que ponía a la venta por primera vez los tokens de DAO (Decentralized Autonomous Organization u Organización Autónoma Descentralizada). Se recaudaron 12,07 millones de ETH (ETH es el código de los ethers como BTC lo es de los bitcoins), más de 150 millones de dólares al cambio. TheDAO era un fondo de capital riesgo abierto donde cualquier persona del mundo podía participar para invertir en proyectos basados en el protocolo Ethereum, automatizados con contratos inteligentes, sin la necesidad de tener una estructura de gestión.

No obstante, TheDAO fracasó porque un hacker logró bloquear 3,6 millones de ethers. Y si bien el problema se resolvió semanas más tarde, provocó una ruptura en la comunidad de Ethereum por la forma en que se había encarado la cuestión. La consecuencia fue la división en dos de la comunidad Ethereum: Ethereum Classic (su token se llama ether classic o ETC) y Ethereum (ETH). Esta crisis, unida a otros problemas técnicos, provocaron la bajada del precio de los ethers desde sus máximos de 21,50 dólares por ether a mediados de junio de 2016 hasta los 7 dólares a finales de ese año. A pesar de esta significativa bajada, la revalorización del ether sólo en 2016 fue del 700%.

El ICO de Z-Cash

En el momento de su aparición en octubre de 2016, el proyecto ZCash (cuya unidad de cuenta es ZEC) recibió el apoyo de más de treinta inversores que aportaron 3 millones de dólares para su desarrollo. La base monetaria es aquí la misma que para bitcoin, 21 millones de unidades. Pero Z-Cash no utilizó el preminado para compensar a sus inversores. Más aun, su protocolo especifica que los mineros sólo podrán hacerse con el 90 % de las monedas y que el 10 % restante está destinado a los inversores (1,65 %), fundadores y empleados de la compañía (5,70 %), e inversiones corporativas (2,65 %). Ese 10 % de las monedas se reembolsará en los cuatro primeros años de vida de Z-Cash. Lo que se busca obrando así es el compromiso de los socios con el proyecto y la estabilidad de la compañía en sus primeros años de andadura.

Las semanas anteriores al lanzamiento de Z-Cash, el precio fue calentándose en el mercado de futuros hasta situarse, a finales de octubre de 2016, en los 3.300 bitcoins por ZEC (unos 2 millones de dólares). En la misma semana, sin embargo, el precio cayó hasta 1 BTC. La razón de estos precios tan altos no es otra que la ley de oferta y demanda: en el mercado inicial había muy pocos ZEC, por lo que su valor subió a cotas irreales, pero a medida que se fueron minando y generándose más monedas, bajó hasta los 60 dólares que alcanzó a finales de 2016.

Los especuladores de ICO

Históricamente, los especuladores de ICO han investigado y seguido los lanzamientos de nuevas criptomonedas con el propósito de adelantarse a los movimientos objetivos del mercado. Los primeros inversores buscaban así beneficiarse de la posterior revalorización que puede darse ante una exitosa comercialización del nuevo token. Una de las características de cualquier ICO para que pueda aumentar rápidamente su precio es la falta de liquidez y oferta en el mercado del token en cuestión. Cualquier especulador que se atreva con este mercado debe ser consciente de esta situación.

Modelos de inversión en criptomonedas

Sólo después de entender las características del mercado de las criptomonedas es posible explorar los caminos que se abren en este campo y participar de sus activos. Los principales modelos de inversión a tener en cuenta son, por un

lado, la inversión en proyectos con alto rendimiento potencial de nuevos protocolos que usan criptomonedas o tokens propios; por otro, la inversión con criptomonedas ya existentes, pero con objetivos diferentes.

En el caso de la inversión en proyectos con criptomonedas nuevas lo que se busca es participar en el potencial futuro de nuevos protocolos descentralizados. Suele llevarse a cabo mediante los denominados ICO (Initial Coin Offering) que hemos explicado antes, bien con blockchains propias o bien con blockchains ya establecidas. Ethereum es uno de los casos de éxito de este sistema. No obstante, existen multitud de proyectos que han deparado pérdidas importantes a los inversores, por lo que conviene afrontar el proceso con conocimiento y buen juicio. Esto es, hay que entender el proyecto, conocer a sus fundadores y desarrolladores, recabar información sobre sus inversores, etc. Si bien existen algunas páginas web que ofrecen información sobre los nuevos ICO y sus condiciones, lo más recomendable es contar con asesoramiento profesional antes de acometer este tipo de inversión.

En lo que se refiere a la inversión con criptomonedas ya existentes, se dan dos tipologías dependiendo de si el objetivo es la especulación o una inversión como parte de una cartera de valores diversificada. Lo explicamos a continuación en más detalle.

Dos tipos de especulación

Esta especulación puede ser de dos tipos. El primero de ellos es el que opera con sistemas automáticos de alta frecuencia (High Frequency Trading, HFT): se trata de una forma de especulación que cobra interés una vez los tokens se ponen en circulación y los diferentes Exchanges los van incorporando en sus plataformas de negociación. Basta ver la evolución del precio de bitcoin para entender que, como si de otro activo se tratase (acción, divisa, bono…), uno puede tomar posiciones especulativas con diferentes objetivos. El activo presenta aquí lo que cualquier especulador demanda: liquidez, volumen, transparencia y facilidad operativa. Es en este momento cuando entran en juego aquellos inversores más sofisticados que, utilizando sistemas automáticos de alta frecuencia, establecen sus parámetros para entrar y salir de las criptomoneda. En este tipo de operativa se utilizan algoritmos de forma automatizada y ordenadores muy sofisticados para ejecutar operaciones en fracciones de segundos. Al existir varios Exchanges

en los que se dispersa todo el volumen, este tipo de implementación resulta algo más laborioso que el equivalente realizado en la compra y venta de acciones, por ejemplo. Sin embargo, esos Exchanges cuentan con API abiertas que permiten una operativa muy sencilla. Esto ha permitido que exista un buen número de operadores que, a partir de los algoritmos que realizan las operaciones de compraventa, encuentran oportunidades de arbitraje y explotan las ineficiencias que se dan en el sistema. Además, dado el bajo coste de realizar cambios en esos algoritmos, adaptarse al mercado es tan económico como sencillo y rápido.

El segundo tipo de especulación recurre a posicionamientos para buscar tendencias. Cuando alguien piensa en tomar posiciones de inversión en cualquier activo, con independencia del plazo, lo primero que debe hacer es establecer una estrategia o plan de inversión: técnicas de valoración, posicionamiento, diversificación, limitación del monto a invertir, precio objetivo, etc. Asimismo, exigirá al activo que tenga un cierto volumen, una buena capitalización y que el número de participantes sea lo más grande posible. Tras esto sigue la estimación de la valoración de la criptomoneda sobre la que se pretende tomar posiciones. En este caso, la estimación vendrá del lado de la curva de demanda, al estar la oferta limitada y ser conocida. Sin duda, es ésta una de las tareas más complejas de todo el proceso. Por último, cada inversor decidirá cómo participar del movimiento de precios. La aplicación de un análisis técnico nos ayudará a definir la tendencia en cada momento de mercado y a intentar predecir el comportamiento más probable del precio, así como los niveles clave que pueden alterar ese comportamiento.

Inversión como parte de una cartera de valores diversificada

Conocidas las técnicas de posicionamiento y especulación, la siguiente ventaja que ofrece el bitcoin es la posibilidad de incorporarlo a una cartera de inversión diversificada como si fuera un activo financiero más. Desde el punto de vista de un gestor que opera en mercados muy líquidos y que desea limitar la volatilidad global e individual de cada componente de la cartera, el bitcoin representa actualmente el único activo digital que se podría utilizar.

La principal razón por la que puede ser interesante incluir el bitcoin en una cartera es que se trata de un activo no correlacionado con los tradicionales y que reacciona a factores tecnológicos y no a los provocados por los mercados

clásicos. Además, sus características específicas de rentabilidad y riesgo ayudan a mejorar, y mucho, la diversificación de una cartera. Para demostrar este punto, analizaremos esta criptomoneda desde la perspectiva de una cartera de valores.

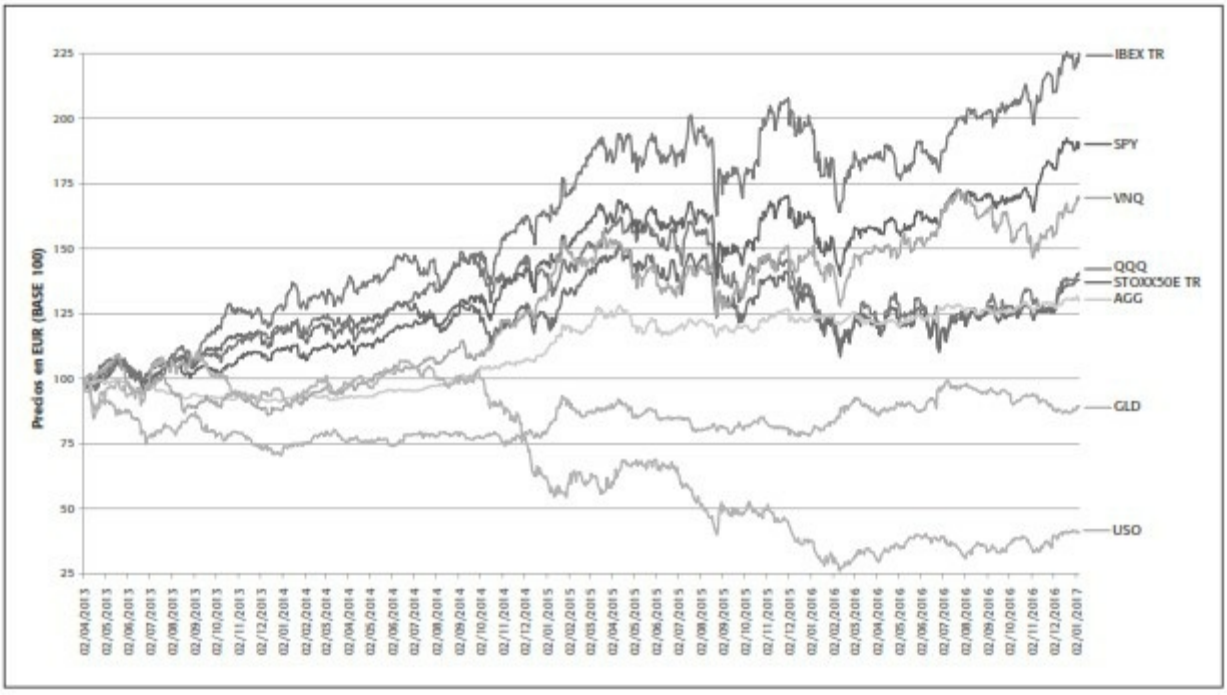
Partiremos de una serie de activos convertidos a euros. El activo con la serie histórica más corta, inaugurada el 19 de julio de 2010, es el bitcoin. Pero dada la evolución del precio desde esa fecha, que distorsiona cualquier cálculo, vamos a eliminar esa parte inicial y partir desde el primer día en que el bitcoin superó los 100 dólares. Fue el 4 de abril de 2013. Todos los activos están ajustados por dividendos, como puede verse en la tabla 5.1.

TABLA 5.1

CÓDIGO (TICKER)	NOMBRE
IBEX TR	Ibex Total Return
STOXX50E TR	Eurostoxx50 Index Total Return
SPY	SPDR SP500 ETF
QQQ	PowerShares QQQ ETF Nasdaq
AGG	iShares Core US Aggregate Bond ETF
VNQ	Vanguard REIT ETF
GLD	SPDR Gold Shares ETF
USO	United States OIL Fund LP ETF
BTCUSD	BTCUSD Bitcoin

La figura 5.1 reproduce una gráfica de precios de todos los componentes analizados, salvo el bitcoin (que necesita de una escala propia), en euros y base 100 en la fecha de análisis:

FIGURA 5.1



A continuación, la figura 5.2 muestra la gráfica de volatilidad de sesenta días anualizada de los ocho activos objeto del estudio y en el tiempo considerado.

FIGURA 5.2

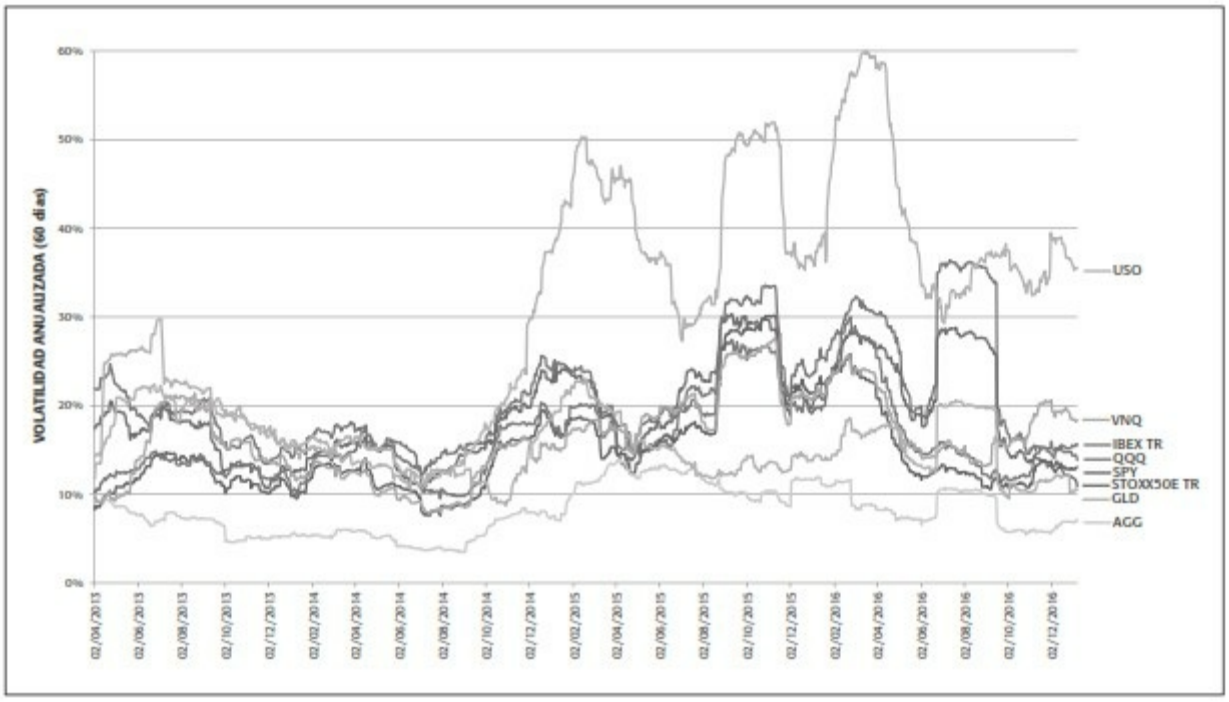
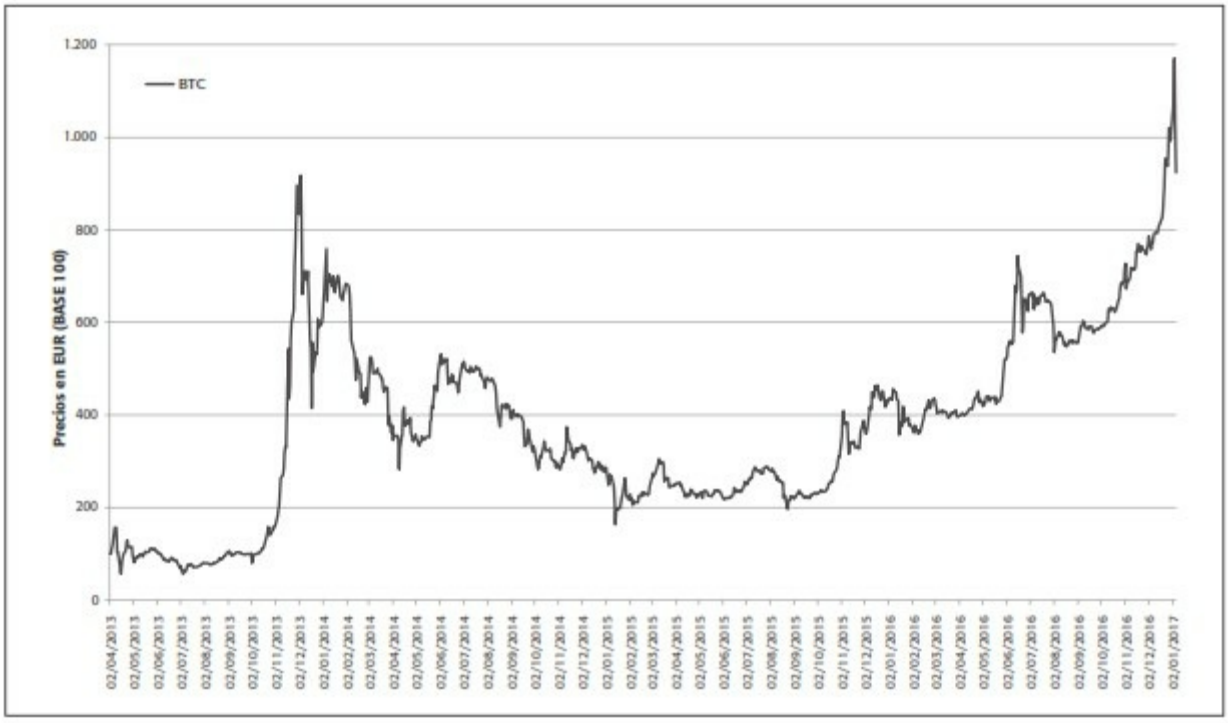
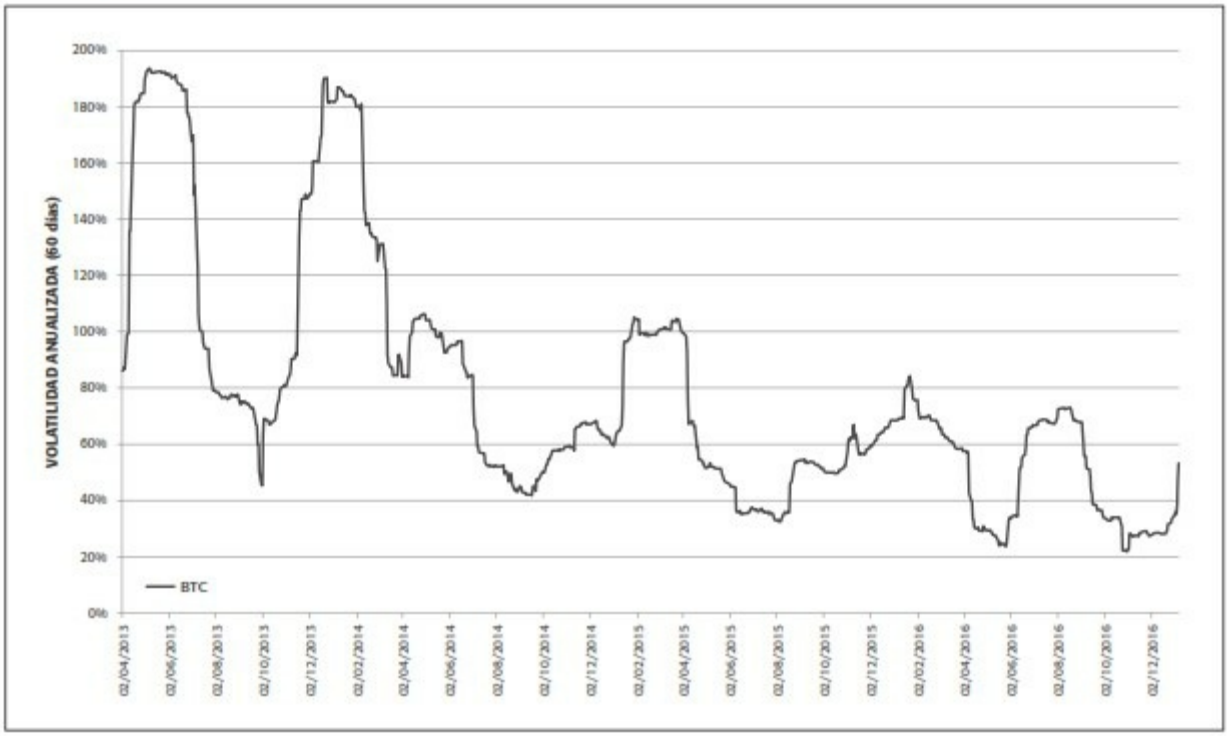


FIGURA 5.3



Si ahora vemos la gráfica de evolución de precios (figura 5.3) y la de volatilidad de sesenta días anualizada del bitcoin (figura 5.4), obtenemos estos datos:

FIGURA 5.4



Lo primero que destaca de estas cuatro gráficas es que tanto la rentabilidad como la volatilidad del bitcoin son ciertamente altas. Sin embargo, esta última muestra una tendencia claramente bajista que está llevando los niveles a rangos mucho más reducidos y similares al de los otros activos arriba considerados. Si tomamos la volatilidad del bitcoin y la comparamos con la que tienen el dólar y el euro, o el oro y el dólar, a sesenta días en datos diarios, vemos que aun siendo mayor, también se aprecia esa convergencia con respecto a esos activos (figura 5.5).

La tabla 5.2 muestra los datos estadísticos de todos los activos contemplados. De todos ellos, el bitcoin es el que presenta la mayor rentabilidad y volatilidad. Destacan también los datos de curtosis y asimetría negativa del bitcoin. La curtosis mide la concentración de datos alrededor de la media. Si ese coeficiente es nulo, la distribución es normal; si es positivo, la distribución es leptocúrtica y significa que los datos se concentran, en mayor medida, en torno a la media. Con la asimetría se identifica si los datos se distribuyen de forma uniforme alrededor de la media. Si es negativa, la mayor cantidad de datos se aglomera en los valores menores que la media.

FIGURA 5.5

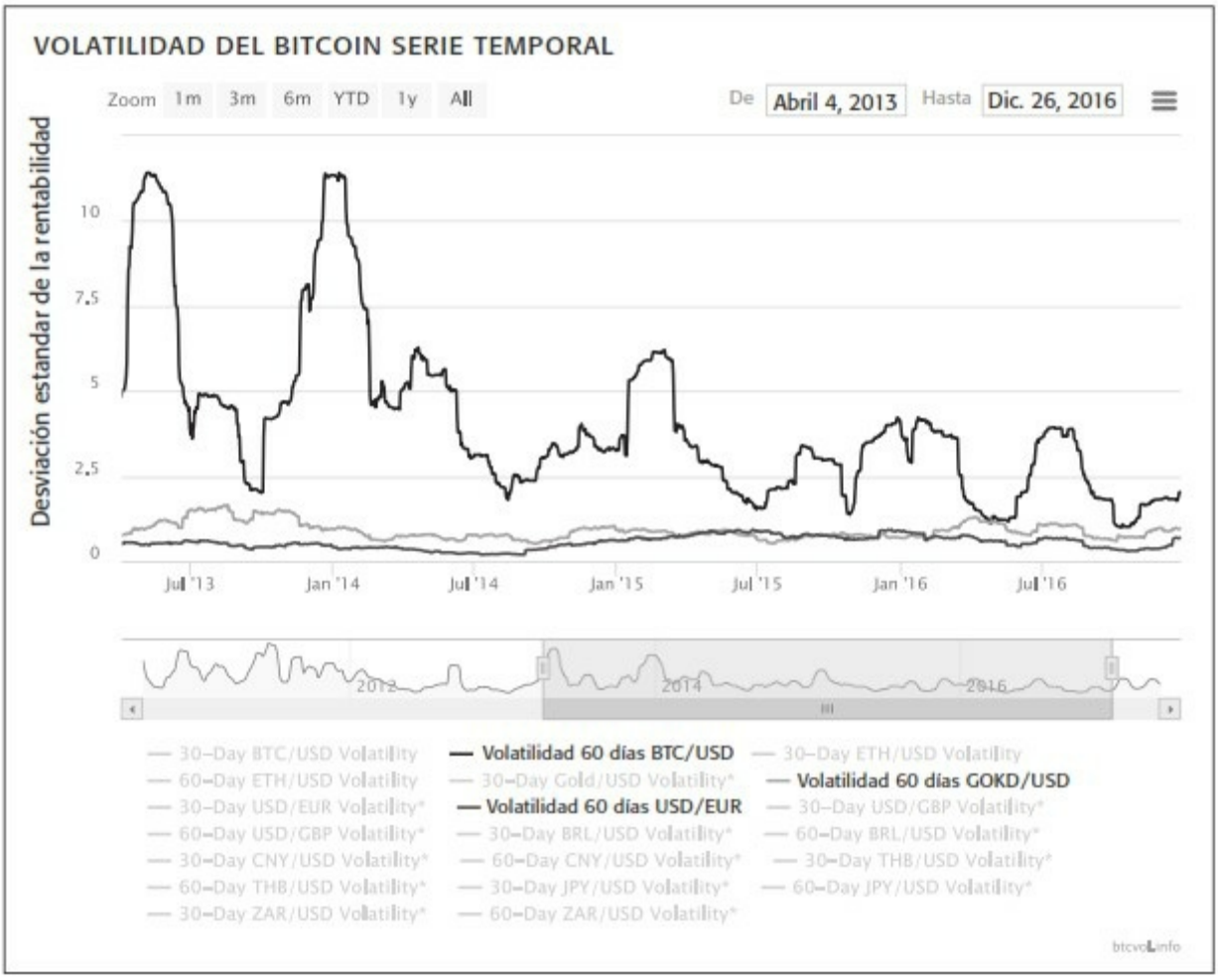

VOLATILIDAD DEL BITCOIN SERIE TEMPORAL
Zoom 1m 3m 6m YTD 1y All
De Abril 4, 2013 Hasta Dic. 26, 2016
Desviación estandar de la rentabilidad
10
7.5
5
2.5
0
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
2012
2014
2016
30-Day BTC/USD Volatility
Volatilidad 60 días BTC/USD
30-Day ETH/USD Volatility
60-Day ETH/USD Volatility
30-Day Gold/USD Volatility*
Volatilidad 60 días GOKD/USD
30-Day USD/EUR Volatility*
Volatilidad 60 días USD/EUR
30-Day USD/GBP Volatility*
60-Day USD/GBP Volatility*
30-Day BRL/USD Volatility*
60-Day BRL/USD Volatility*
30-Day CNY/USD Volatility*
60-Day CNY/USD Volatility*
30-Day THB/USD Volatility*
60-Day THB/USD Volatility*
30-Day JPY/USD Volatility*
60-Day JPY/USD Volatility*
30-Day ZAR/USD Volatility*
60-Day ZAR/USD Volatility*
btcvol.info

TABLA 5.2

	IBEX TR	STOXX50E TR	SPY	QQQ	AGG	VNQ	GLD	USO	BTC
StartDate:	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013
EndDate:	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017
Perfomance:	38,75%	37,16%	87,06%	123,93%	28,10%	64,81%	-9,55%	-60,61%	805,65%
TAE:	8,99%	8,66%	17,89%	23,60%	6,72%	14,03%	-2,60%	-21,71%	78,43%
VOL:	20,98%	19,58%	15,94%	18,12%	8,47%	17,32%	16,51%	33,66%	88,97%
MaxDrawDown (%):	-32,31%	-28,37%	-18,00%	-21,03%	-9,38%	-20,58%	-29,64%	-76,37%	-82,19%
MaxDrawDown (nDays):	304	304	72	70	133	158	272	887	406
Sharpe:	0,42	0,44	1,11	1,30	0,79	0,81	-0,16	-0,65	0,88
Sortino:	0,54	0,59	1,56	1,76	1,12	1,10	-0,21	-0,95	1,02
Skewness:	-1,17	-0,54	-0,24	-0,29	-0,18	-0,39	-0,33	0,13	-0,12
Excess Kurtosis:	9,89	3,53	3,40	3,39	4,89	2,29	8,30	2,16	15,76

En la tabla 5.3 vemos cómo el bitcoin se beneficia de una casi nula correlación con el resto de activos. Sólo en el caso de los bonos (AGG) vemos un 13% de correlación.

El siguiente cálculo que llevamos a cabo consiste en investigar el impacto, en términos de rentabilidad y riesgo, de la inclusión del bitcoin en una cartera. Sólo se consideran posiciones largas. Tomamos los mismos activos y plazos anteriores y siempre convertidos a euros.

Supongamos ahora que se construye una cartera A compuesta por ocho activos (todos excepto el bitcoin). Empezamos con una cartera equiponderada, es decir, una en la que todos los activos tienen el mismo peso inicial dentro de la cartera. Al final de cada semestre realizamos el rebalanceo semestral de la cartera. Una vez establecidos los pesos iniciales, dejamos a la cartera fluctuar libremente en el mercado, de tal forma que los componentes con tendencia alcista irán ganando mayor peso dentro de ella. Cada seis meses (en el último día hábil de junio y diciembre) rebalancearemos la cartera para volver a asignar los pesos iniciales a cada uno de sus componentes. De esta forma tratamos de mantener estables los pesos de cada activo sin incurrir en muchos gastos de brokerage.

Imaginemos ahora que construimos una cartera B compuesta por los nueve activos (todos, incluido el bitcoin) y seguimos exactamente el mismo proceso, incluido el rebalanceo semestral. La evolución gráfica de las carteras y de su volatilidad de 2013 a 2016 sería la que muestran la figura 5.6 y la figura 5.7.

Claramente se aprecia que el incremento de volatilidad aportado por la inclusión del bitcoin se compensa con un extra de rendimiento. El efecto de descorrelación con el resto de activos tradicionales es obvio y mejora la diversificación sensiblemente. Sin embargo, colocar un 11% en bitcoins resulta excesivo, por lo que debería limitarse el peso de esta criptomoneda en la cartera.

TABLA 5.3. Matriz de correlaciones

	IBEX TR	STOXX50E TR	SPY	QQQ	AGG	VNQ	GLD	USO	BTC
IBEX TR	1	0,9206	0,5046	0,4620	0,0862	0,3273	-0,0929	0,2731	0,0352
STOXX50E TR	0,9206	1	0,5819	0,5395	0,1681	0,3898	–0,0715	0,2759	0,0251
SPY	0,5046	0,5819	1	0,9468	0,5246	0,7265	0,0799	0,3771	0,0630
QQQ	0,4620	0,5395	0,9468	1	0,4904	0,6597	0,0605	0,2945	0,0566
AGG	0,0862	0,1681	0,5246	0,4904	1	0,5212	0,3024	0,0994	0,1278
VNQ	0,3273	0,3898	0,7265	0,6597	0,5212	1	0,1821	0,1683	0,0377
GLD	–0,0929	–0,0715	0,0799	0,0605	0,3024	0,1821	1	0,1050	0,0724
USO	0,2731	0,2759	0,3771	0,2945	0,0994	0,1683	0,1050	1	0,0103
BTC	0,0352	0,0251	0,0630	0,0566	0,1278	0,0377	0,0724	0,0103	1

FIGURA 5.6

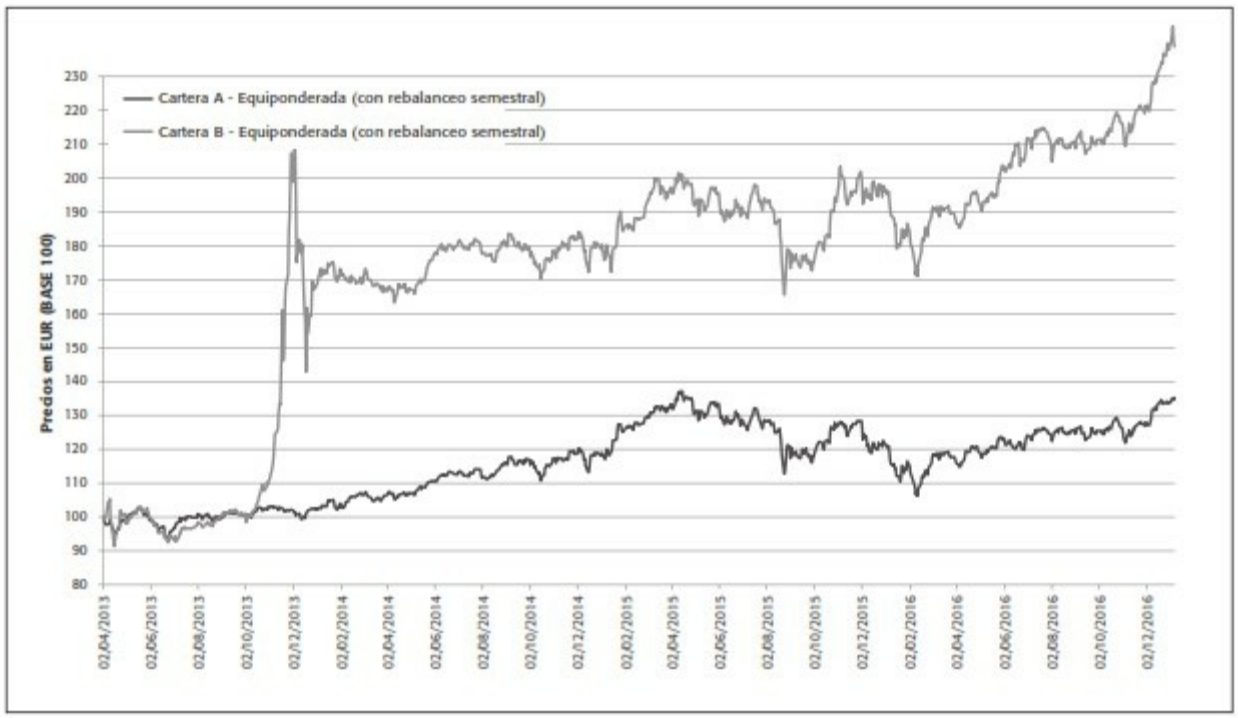
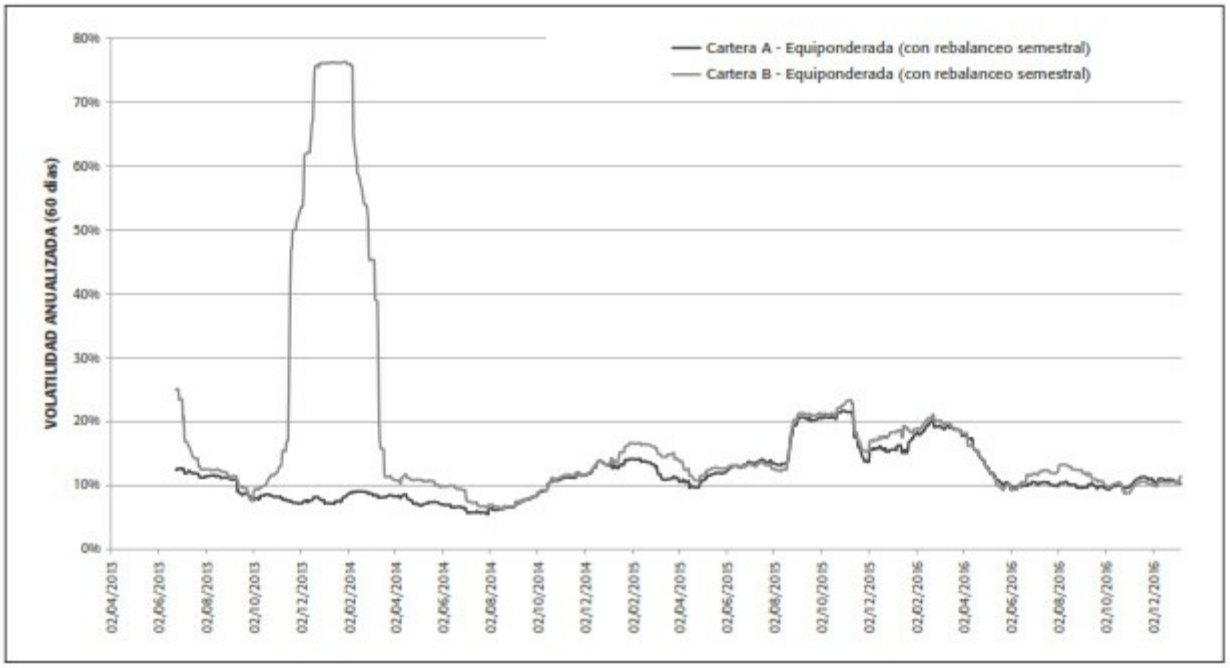


FIGURA 5.7



Para terminar de demostrar si el bitcoin aporta valor o no en la gestión de carteras vamos a ver a continuación cómo quedaría dentro de una frontera eficiente. Entre las limitaciones que aquí hay que considerar está la de que el bitcoin presenta una distribución de retornos leptocúrtica y que los métodos de optimización de media/varianza son muy sensibles a los inputs, pero es una forma válida para visualizar los efectos de las particularidades de este activo. En

la cartera óptima de la frontera eficiente, que es aquella con la mínima varianza, lógicamente no se incluirá el bitcoin. Sin embargo, a poco que el inversor decida asumir un poco de riesgo, logrará un salto muy importante de rentabilidad. Los cálculos de la tabla 5.4 se realizan bajo unos supuestos de pesos máximos del 1%, 1,5%, 2% y 5% con el fin de limitar la exposición.

Lo que gráficamente se traduciría en la figura 5.8.

A medida que incorporamos más bitcoins a la cartera es verdad que sube su riesgo, pero con un incremento sustancial de rentabilidad. De esa forma y, con respecto a la cartera eficiente que no incorpora BTC, el colocar un 1 % hace saltar la TAE desde poco más del 7 % al 13 %, siendo el incremento de la volatilidad anualizada del 8 % al 9,6 %. Son datos que justifican la introducción de un pequeño porcentaje de bitcoins. Gráficamente ésta hubiera sido la evolución de las diferentes carteras analizadas (figura 5.9) y de su volatilidad (figura 5.10).

FIGURA 5.8

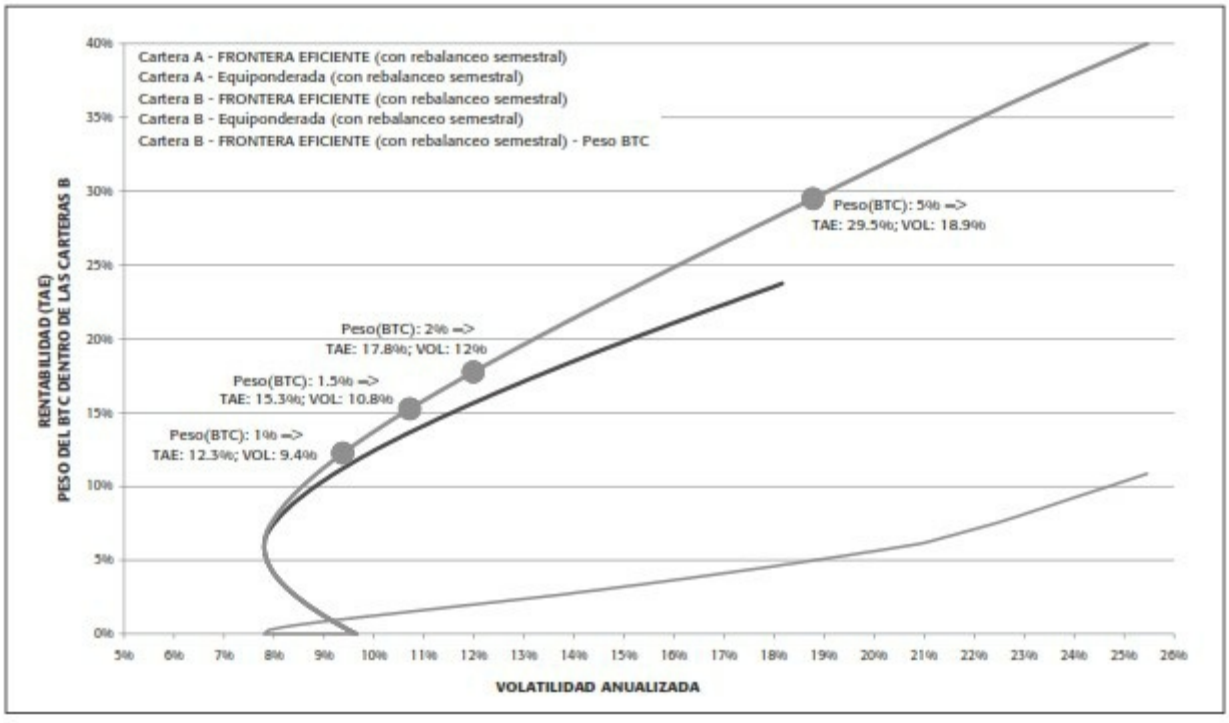
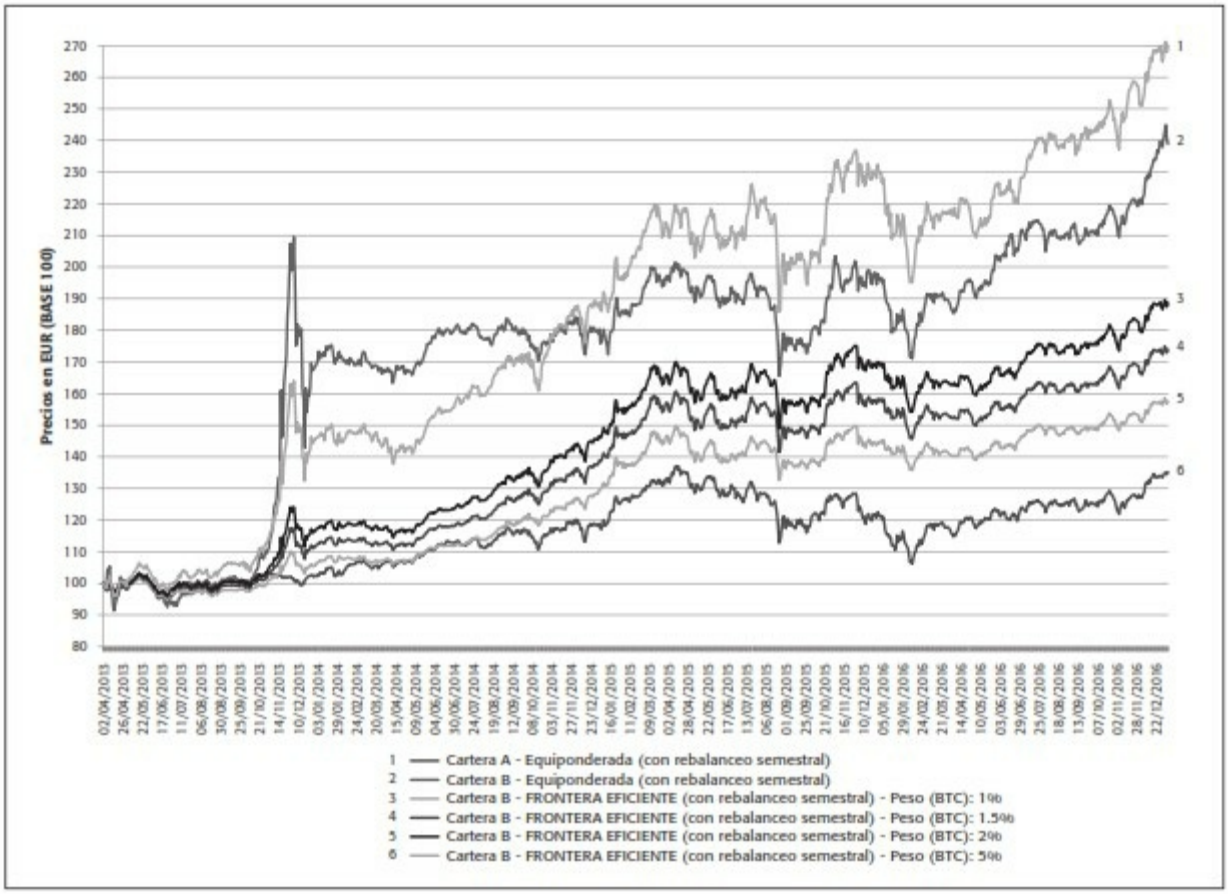


TABLA 5.4

	Cartera A 8 activos Equiponderada (con rebalanceo semestral)	Cartera B 9 activos Equiponderada (con rebalanceo semestral)	Cartera B 9 activos FRONTERA EFICIENTE Peso (BTC): 1% (con rebalanceo semestral)	Cartera B 9 activos FRONTERA EFICIENTE Peso (BTC): 1,5% (con rebalanceo semestral)	Cartera B 9 activos FRONTERA EFICIENTE Peso (BTC): 2% (con rebalanceo semestral)	Cartera B 9 activos FRONTERA EFICIENTE Peso (BTC): 5% (con rebalanceo semestral)
StartDate:	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013	02/04/2013
EndDate:	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017	20/01/2017
Performance:	33,30%	135,34%	55,31%	71,62%	86,38%	167,79%
TAE:	7,85%	25,22%	12,26%	15,25%	17,78%	29,54%
VOL:	12,11%	23,43%	9,41%	10,75%	12,04%	18,88%
MaxDrawDown (%):	–22,53%	–31,85%	–11,43%	–11,99%	–12,53%	–17,65%
MaxDrawDown (nDays):	304	14	133	133	133	70
Sharpe:	0,64	1,08	1,30	1,42	1,48	1,56
Sortino:	0,90	1,31	1,78	1,92	1,99	2,04
Skewness:	–0,40	1,28	–0,39	–0,32	–0,25	0,02
Excess Kurtosis:	2,98	44,41	3,47	3,63	4,13	8,26

FIGURA 5.9

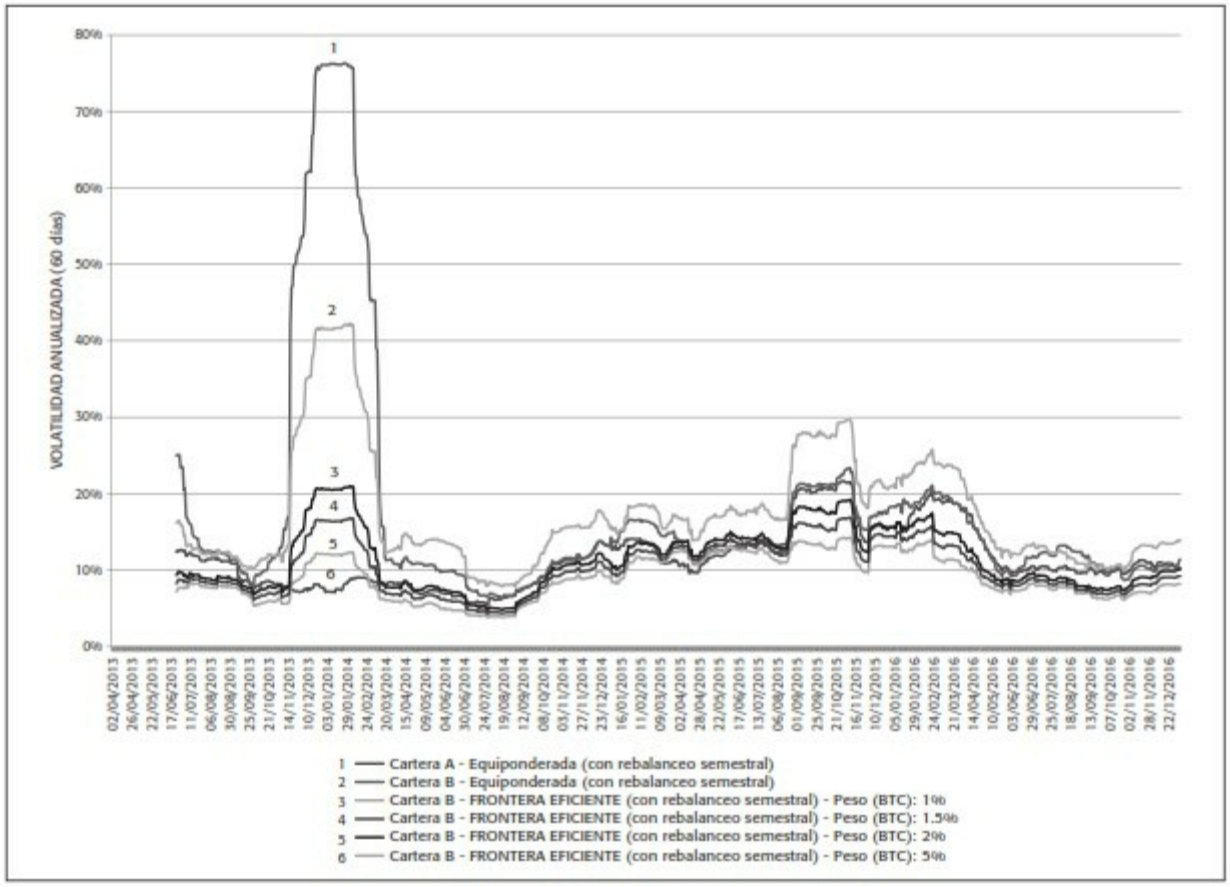


Asimismo, el cálculo para la cartera con un 1% de BTC del CVaR (99%) a un día, que es la pérdida media esperada si caemos en uno de esos días que entran dentro del 1 % de los peores días sería la que muestra la tabla 5.5.

TABLA 5.5

VaR (empírico) 1 día:	−1.78 %	−1.36 %	VaR (teórico) 1 día
CVaR (99 %) 1 día:	−2.24 %		

FIGURA 5.10



El VaR (Value at Risk) es un método para cuantificar el riesgo que mide la máxima pérdida esperada en un intervalo de tiempo determinado, en condiciones normales del mercado y para un nivel de confianza dado. Con el CVaR (Conditional Value at Risk) analizamos los rendimientos inferiores al VaR.

Desde el punto de vista de un inversor, la quizá sorprendente conclusión es que el incorporar bitcoins en una cartera de valores proporciona una alta rentabilidad que compensa, y con creces, el mayor riesgo asumido. Además, logra mejorar la diversificación y debería ser considerada por la comunidad inversora como un activo financiero más a utilizar.

Para más información actualizada sobre inversiones en criptomonedas de las blockchains públicas en <libroblockchain.com/inversion/>.

Capítulo 6

Aspectos legales de los ICO, Smart Contracts y DAO

Xavier Foz Giralt, Joaquim Matinero Tor, José Ramón Morales Cáceres y Cristina Carrascosa Cobos

La tecnología blockchain suscita dudas a nivel legal que tardarán tiempo en encontrar respuesta, sobre todo en lo que se refiere a sus aplicaciones más innovadoras, como las Initial Coin Offerings (ICO), los Smart Contracts o las Decentralized Autonomous Organizations (DAO). Estos conceptos, y otros nuevos que irán surgiendo en el futuro, tendrán que adecuarse a un marco regulador. En las siguientes páginas vamos a ver los problemas legales que plantean y cómo solucionarlos.

La problemática legal de las Initial Coin Offerings (ICO)

En la sección de este libro sobre cómo invertir en criptomonedas hemos explicado los instrumentos y características de una Initial Coin Offering (ICO), también denominada *token crowdsale*. Pero en este espacio no vamos a incidir en su funcionamiento, sino en la incertidumbre regulatoria que hay alrededor de una figura que presenta características que podrían encajar en distintas categorías jurídicas, como la oferta pública de valores, el crowdfunding o incluso en esquemas de inversión colectiva.

La denominación de ICO tiene que ver con lo que en términos anglosajones se conoce como Initial Public Offering (IPO), esto es, una oferta pública de un valor. La principal duda, aún no resuelta ante la falta de pronunciamiento tanto por parte del regulador nacional —la Comisión Nacional del Mercado de Valores (CNMV) en España— como de sus homólogos internacionales —en particular, el estadounidense SEC y el británico FCA—, es si los tokens pueden ser conceptualizados como un valor. En España, a la luz de la normativa vigente en 2017 —contenida en la Ley del Mercado de Valores— que define los instrumentos financieros, nos encontramos con un concepto

genérico de valor negociable. Éste comprende cualquier derecho de contenido patrimonial, cualquiera que sea su denominación, que por su configuración jurídica propia y régimen de transmisión sea susceptible de tráfico generalizado e impersonal en un mercado financiero. No obstante, ninguno de los instrumentos descritos en el listado ejemplificativo que prevé dicha ley encaja propiamente con el objeto de una ICO.

No estamos, en efecto, ni ante un valor participativo, como podría ser una acción o un valor negociable equivalente, ni tampoco ante un instrumento del mercado monetario asimilable a un pagaré, ya que no hay una representación de una deuda exigible a un emisor. Tampoco parece posible asimilarlo a los contratos de instrumentos financieros derivados relacionados con divisas, ya que la Dirección General de Tributos considera las criptomonedas como un medio de pago y no como dinero en sí mismo.

Así las cosas, hay una corriente que, precisamente para escapar del riguroso marco regulatorio que sería de aplicación a las ICO si se considerasen ofertas públicas de valores, aboga por enmarcarlas en la categoría de crowdfunding y, más concretamente, en el de donación o recompensa. Sus defensores sostienen que estaríamos bien ante una especie de donación por el trabajo realizado por los desarrolladores o bien ante una aportación a través de la cual lo que se obtendría sería un producto o servicio asimilable a una licencia de software. Aunque pueden existir argumentos a favor de considerar esta opción, creemos que va a ser difícil convencer a los reguladores de que las personas que suscriben estos tokens no están esperando obtener un rendimiento dinerario que va más allá de una donación altruista o de la precomercialización de un determinado producto o servicio. En cualquier caso, tampoco la normativa española reguladora del crowdfunding en España ofrece pautas útiles para aclarar este fenómeno. Por un lado, la regulación existente de las plataformas de financiación participativa excluye expresamente de la misma la captación de financiación a través de donaciones o venta de bienes y servicios, y, por otro, las formas permitidas de captación de fondos bajo dicha normativa (a saber, la emisión de obligaciones, acciones o participaciones o la solicitud de préstamos) no son asimilables a esta figura según hemos visto.

Como último apunte, cabe mencionar también la posibilidad de que estructuras como TheDAO pudieran ser consideradas como entidades de inversión colectiva de tipo cerrado (que engloban, por ejemplo, a las entidades de capital riesgo) y, por tanto, sujetas a la regulación de la CNMV. Tiene sentido si se tiene en cuenta que obtienen capital de una serie de inversores mediante una actividad comercial, cuyo fin es generar ganancias o rendimientos mediante una política de inversión definida. En este caso, la inversión en proyectos de startups relacionados con la tecnología blockchain.

A la vista de todo ello, y sin descartar que tarde o temprano las legislaciones y los reguladores nacionales intenten acometer medidas en aras a la protección de los inversores (lo cual no será fácil por las características globales y descentralizadas de las ICO), la reglamentación ahora mismo de estas ofertas debe pasar por su autorregulación y, en particular, por la implementación de determinadas buenas prácticas en la emisión y el establecimiento de procedimientos de gobierno corporativo que den confianza a los inversores y redunden en la credibilidad y reputación de los proyectos que recurren a este mecanismo para levantar financiación. En este sentido, el hecho de que el emisor sea una entidad jurídica debidamente constituida en una jurisdicción de la OCDE, la puesta a disposición de los inversores de un whitepaper exhaustivo que contenga una descripción sólida del proyecto y de sus promotores, la existencia de un documento de suscripción estándar, la realización de una *due diligence* previa y, sobre todo, la presencia de un agente verificador independiente que monitorice el destino de los fondos mediante la creación de *escrows* o monederos multifirma que requieran su intervención son elementos clave que, a falta de regulación, pueden garantizar un entorno transparente y seguro para los inversores en este tipo de proyectos.

Los contratos inteligentes desde un punto de vista legal

El término Smart Contracts puede designar desde contratos o cláusulas contractuales en lenguaje natural trasladados a código informático hasta casos más complejos representados y ejecutados directamente por scripts. Aunque los Smart Contracts se pueden utilizar en entornos de interacción diferenciados, cada uno generador de retos jurídicos muy diversos, en este espacio nos

centraremos en aquellos que se utilizan para canalizar transacciones comerciales, y ello a la luz del sistema legal español. En todo caso, cuestiones similares se plantean también en otros países de nuestro entorno.

El mundo legal y comercial actual de la contratación se basa en premisas que no acaban de encajar con la forma de operar de los Smart Contracts. Para valorar su impacto en los negocios y sus riesgos e implicaciones legales será preciso que el fenómeno alcance una mayor madurez y se consolide su utilización a escala suficiente (al menos en algunos casos de uso). Sólo de ese modo será posible identificar las buenas prácticas y que los reguladores y los tribunales alcancen el grado de comprensión y familiaridad necesarios. Entretanto, el uso de Smart Contracts para la contratación comercial se mueve en la incertidumbre jurídica. Además, los problemas jurídicos de la utilización de un Smart Contract pueden variar sustancialmente dependiendo de si operan en un entorno de blockchain pública o si lo hacen en una blockchain privada.

La cuestión previa que resolver es cómo elaborar y qué condiciones debería reunir un Smart Contract para ser considerado un acuerdo legalmente vinculante y exigible ante los tribunales desde el punto de vista de las normas sobre contratación. Para empezar, es necesario que reúna los requisitos legales esenciales de todo contrato, es decir: que concurra el consentimiento de las partes, que tenga un objeto lícito y una causa (motivo válido, incluyendo la contraprestación).

Los límites legales de la libertad contractual

Nuestro entorno legal concede a las partes un amplio margen para alcanzar acuerdos y contratar libremente en los términos que consideren. Pero esta libertad contractual está sujeta a límites legales: prohibiciones para determinados contratos por razón de su objeto —bien por ser objeto ilícito o contrario al orden público— o restricciones sobre qué se puede y qué no se puede pactar, como sucede en contratos con consumidores o en contratos de trabajo. Los límites legales a la libertad de contratación deberán respetarse también en un Smart Contract para que éste se considere válido y legalmente exigible.

La lógica de autoejecución condicionada propia de los Smart Contracts encajaría bien con la posibilidad, prevista en la ley, de someter los contratos a una condición, que puede configurarse bien como condición suspensiva (la obligación prevista resulta exigible o el derecho se transfiere sólo a partir de que se produzca la condición) o bien como condición resolutoria (el derecho se transfiere o la obligación empieza a surtir efectos desde la firma, pero dejará de tener efectos si se cumple la condición reflejada en el contrato).

Existen condiciones contractuales relativamente sencillas de formular en lenguaje de programación y que el propio Smart Contract puede verificar, bien valiéndose de fuentes confiables dentro de su propio entorno blockchain o fuera de él (el oráculo externo), o bien con la aportación de determinados documentos de contenido tasado, un requisito habitual para ejecutar un contrato de *escrow* o un crédito documentario. Pero la contratación comercial a menudo contiene condiciones poco aptas para su utilización como detonante de la ejecución de un Smart Contract, ya sea porque la condición no es susceptible de representación y ejecución mediante código, o porque la verificación de su cumplimiento se presta a interpretación. En estos casos, para construir un acuerdo legalmente vinculante y exigible, habrá que acudir a soluciones mixtas que combinen previsiones en código con otras en lenguaje natural. Esto es lo que ocurre, por ejemplo, en el sistema de Smart Contracts Corda del consorcio R3. Además, también en un Smart Contract deberían respetarse las restricciones legales relativas al tipo de condiciones admisibles. Así, legalmente no cabría sujetar una obligación a una condición que resulte imposible, contraria a las buenas costumbres o prohibida por la ley (en esos casos la obligación resulta nula); ni sería admisible tampoco que el cumplimiento de la condición dependa sólo de la voluntad del que asume la obligación. Por ello, en un Smart Contract debe evitarse designar como oráculo a una fuente que esté bajo el control de la parte obligada.

En general, la ley admite la libertad de forma de los contratos, salvo en los casos específicos en que se exija una forma concreta: forma escrita o en escritura pública. Nuestro sistema legal incluso reconoce que el contrato en soporte electrónico cumple el requisito de forma escrita. Es decir, que ya no es preciso que esté en soporte papel. Pero dicho reconocimiento legal proviene de la directiva europea de comercio electrónico del año 2000, que se elaboró

teniendo a la vista un modelo de comercio electrónico basado en la contratación web, y en ella, aunque los términos contractuales se escriban en código, su contenido debe ser legible en lenguaje natural que sea comprensible para los que contratan. Difícilmente los Smart Contracts redactados sin expresión en lenguaje natural cumplirán con estos requisitos y, sobre todo, con la exigencia de que los términos contractuales hayan sido conocidos y aceptados por las partes fuera de entornos altamente técnicos.

También supone un reto legal la pretendida existencia de Smart Contracts en los que no intervienen personas físicas o jurídicas, dado que la ley únicamente admite la contratación entre personas (sujetos de derecho). En realidad, cuando se habla de transacciones entre dispositivos conectados en el entorno del internet de las cosas o de transacciones realizadas por agentes de software, a efectos jurídicos siempre habrá que buscar quién es el sujeto —persona física o entidad— bajo cuyo control actúa el dispositivo o agente, así como los derechos, obligaciones y responsabilidades por su funcionamiento en el entorno de Smart Contracts que acabarán siendo atribuidos legalmente a dicha persona. Se trata de un debate jurídico complejo que se halla todavía lejos de haberse resuelto.

La contratación en un entorno transaccional descentralizado

Para que un Smart Contract aporte verdadera seguridad jurídica resulta esencial testar si el entorno de transacciones fiables entre partes que no se conocen en una red abierta y sin un intermediario centralizado reúne los requisitos necesarios para constituir prueba suficiente del consentimiento sobre el contenido de lo acordado. Esto requiere tener la certeza razonable de que los registros del ledger de un entorno blockchain pueden constituir una evidencia irrefutable ante los tribunales y demostrar la realización de una transacción en una fecha concreta, entre esas partes concretas y con ese contenido preciso. En este sentido, es esencial que permitan:

- Acreditar la identidad de las partes participantes y sus atributos (por ejemplo, si tienen la edad y la capacidad para contratar, o facultades para representar a la empresa en nombre de la que firman). Aunque la utilización de sistemas de criptografía asimétrica puede aportar seguridad y reforzar la

autenticidad de la transacción, habrá que ver si los sistemas de gestión de identidad en entornos blockchain abiertos y seudoanónimos serán admitidos por los tribunales en caso de repudio de una de las partes.

- Acreditar la integridad de los registros de la transacción, dando prueba suficiente de que su contenido (incluyendo el momento temporal de su formalización) no puede haber sido alterado con posterioridad a su creación. Se atribuye a las plataformas blockchain la capacidad de garantizar la inmutabilidad e impedir la manipulación a posteriori de las transacciones. Pero el marco legal que regula la autenticación de transacciones electrónicas (normativa española sobre firma electrónica, y reglamento europeo eIDAS de 2014 sobre identificación electrónica y servicios de confianza) se basa en la existencia de proveedores de servicios de certificación o proveedores de servicios de confianza que acreditan —con distintos niveles de fuerza probatoria— identidades electrónicas y transacciones. Y no resulta claro si las plataformas blockchain abiertas encajan en dicho marco normativo ni si podrían llegar a ser reconocidas por los reguladores o por los tribunales como entidades de certificación o proveedores de servicios de confianza.

Estas incertidumbres legales serán menores en el caso de Smart Contracts utilizados en las blockchains privadas: el administrador de la plataforma podría mantener un grado de control mayor sobre la identidad de los usuarios y sus atributos, y asegurarse de que consienten en vincularse con los mecanismos de autenticación proporcionados por la plataforma (en el sentido del art. 3.10 de la Ley Española de Firma Electrónica de 2003). Incluso cabría que el administrador de la plataforma asumiera roles propios de una entidad de certificación o de un proveedor de servicios de confianza, permitiendo con ello reforzar la eficacia probatoria de los registros de las transacciones realizadas por las partes.

Para evaluar la capacidad de exigir legalmente el cumplimiento del Smart Contract conviene tomar con cautela su autoejecutabilidad, más allá de simples operaciones de pago u órdenes de venta electrónicas sujetas a condiciones de fácil verificación. Determinadas previsiones o prestaciones de un Smart Contract pueden no ser cumplidas o ejecutadas con la simple interacción del código dentro del ledger, por afectar a activos que son ajenos al mismo, o porque su cumplimiento dependa de condiciones complejas, subjetivas o indeterminadas

que requieran de interpretación experta. En estos casos se podría entender que será necesario un cumplimiento híbrido que requiera tanto de órdenes o movimientos de valor dentro de la plataforma blockchain como de otras que se producen en el exterior de la misma. Y para estas últimas posiblemente sea necesario el recurso a personas o mecanismos externos a la plataforma que auxilien para hacer posible el cumplimiento de todo lo previsto en el Smart Contract.

Lo que resulta esencial es saber en qué medida, si se incumple lo previsto en el Smart Contract por disfunciones en el mismo (en su programación, en el funcionamiento del código o de la plataforma) o por las obligaciones que deben ejecutarse fuera de la plataforma, podrá una de las partes acudir a los tribunales para reclamar su cumplimiento. Para ello, además de ver si concurren los requisitos para la existencia y validez del contrato mencionados en los párrafos anteriores, será necesaria una evolución del marco legal y la práctica judicial a partir de una mayor maduración y extensión en el uso y adopción de los Smart Contracts. Entretanto, nos moveremos en un entorno de incertidumbre legal.

A estas dudas jurídicas hay que añadir la dificultad de determinar cuál es la ley nacional aplicable para evaluar y hacer cumplir el Smart Contract, especialmente en plataformas blockchain abiertas en las que los participantes proceden de distintas jurisdicciones. Las normas internacionales contienen para determinarlo reglas que suelen dar prioridad a lo que acuerden las partes sobre la ley a la que sujetan el contrato. Pero no siempre el acuerdo entre las partes evitará la aplicación de normas imperativas de otras jurisdicciones, como las normas locales de protección del consumidor.

Todo lo dicho hasta ahora no agota la lista de retos jurídicos que plantean los Smart Contracts basados en plataformas blockchain. A modo de ejemplo, podemos citar otras cuestiones que también se mencionan frecuentemente al respecto:

- El cumplimiento de requisitos regulatorios específicos de formalización o de supervisión e inspección del Smart Contract por parte de autoridades regulatorias (por ejemplo, bancarias, del mercado de capitales o sanitarias).

- El riesgo de utilización de Smart Contracts en plataformas blockchain abiertas y seudoanónimas para realizar transferencias de valor o activos fuera de los circuitos habituales del sector financiero, eludiendo así los controles legales de prevención del blanqueo de capitales y la financiación del terrorismo, o las normas sobre sanciones financieras internacionales. Una cuestión esta que está sobre la mesa sobre todo a raíz de la actuación de las autoridades estadounidenses contra el marketplace de la web profunda Silk Road, en la que se detectó una amplia utilización de determinadas criptomonedas para la adquisición de ciertos productos de tráfico ilícito.
- Las responsabilidades por posibles problemas de funcionamiento operativo de un Smart Contract o por brechas de seguridad de la plataforma.
- Las cuestiones que surgen en cuanto a la normativa de protección de datos de carácter personal, como la dificultad de identificar al encargado de tratamiento o los potenciales riesgos de realizar inadvertidamente transferencias internacionales de datos a través de los nodos de la plataforma sin cumplir con las exigencias legales.
- La sujeción a otras normas relevantes como las de derecho de la competencia o las tributarias.

El uso de Smart Contracts no ha alcanzado todavía suficiente nivel de madurez y adopción. Sólo a medida que se acumule experiencia práctica en el mercado y en la actividad regulatoria y judicial podremos contar con un grado razonable de certidumbre legal en relación con su utilización. En cualquier caso, sí que parece altamente aconsejable que tanto en el diseño de plataformas y de programas como en la ejecución de cada Smart Contract participen profesionales con habilidades jurídicas suficientes para asegurar su validez y eficacia legal.

Todo esto exigirá de los abogados nuevos perfiles y habilidades que les hagan capaces de asesorar debidamente en procesos de contratación en entornos de Smart Contracts.

Los retos legales de la DAO

Si los retos e incertidumbres legales para los Smart Contracts y las ICO son grandes desde un punto de vista legal, las DAO (Decentralized Autonomous Organizations u Organizaciones Autónomas Descentralizadas) son el paso siguiente, tal como se explica en la sección de aplicaciones transversales del libro. Como las IIC (Instituciones de Inversión Colectiva), las DAO son colectividades que tienen como objetivo principal «la captación de fondos, bienes o derechos del público para gestionarlos e invertirlos en bienes, derechos, valores y otros instrumentos».[110] En el caso de los fondos de inversión, que como las DAO son entidades sin personalidad jurídica, la ley establece que su representación y gestión corresponde a una gestora. Sin embargo, en las Organizaciones Autónomas Descentralizadas, la gestora y la entidad que capta fondos es todo uno. Los participantes que aportan el capital son a su vez quienes deciden, a través de votaciones y consenso, en qué se invierte el mismo. Por ello, carecen de la «profesionalización» y la seguridad jurídica de que sí están dotadas las IIC, y tampoco están sometidas en principio a la supervisión ni de la Comisión Nacional del Mercado de Valores ni de ningún otro organismo.

Por otro lado, se pueden llegar a parecer a una sociedad anónima tal y como aparece regulada en el Real Decreto Legislativo 1/2010 de 2 de julio, por el que se aprueba el Texto Refundido de la Ley de Sociedades de Capital, pues, por ejemplo, la aportación de fondos da como contravalor una serie de derechos,[111] concretamente el de voto. No obstante, una DAO no gozará de la limitación de responsabilidad que proclama la misma, simplemente porque no está recogida dentro de su ámbito objetivo de aplicación.

Todo en una DAO se sostiene sobre la base de la figura del contrato inteligente, al que da forma un código que, una vez se ejecuta, es irreversible. Como se afirma de forma unánime en el mundo blockchain, ese código es ley. Si la llevamos a nuestro ordenamiento jurídico, una DAO da la sensación de ser un fondo de inversión cuyo consejo de administración lo constituye el código que compone el contrato inteligente y cuya junta de socios toma las decisiones por mayoría, pues la aportación de fondos conlleva el derecho de voto, como si se tratara de cualquier socio capitalista. En palabras del fundador de Ethereum, Vitalik Buterin, la idea al diseñar estas DAO era la de «codificar la declaración

de la misión en un código; es decir, crear un contrato inviolable que genera ingresos, paga a la gente por realizar alguna función y encuentra por sí mismo el hardware donde ejecutarse, todo ello sin necesidad de dirección humana».

TheDAO Project constituye un proyecto formado por una DAO y creado por el equipo de Slock.it[112] para la gestión descentralizada de fondos. Unirse a la DAO es libre, basta con aportar fondos (ethers en este caso), a cambio de los cuales se dan unos derechos de voto digitalizados que, junto con los del resto de participantes, se gestionan en función del consenso que se alcanza. En el momento de su creación, TheDAO consiguió reunir 150 millones de dólares, alcanzando más tarde unos 22.000 participantes en todo el mundo y convirtiéndose de hecho en un proyecto de crowdfunding histórico al superar el récord en recaudación de fondos. La intención del proyecto era intervenir en oportunidades de negocio, así como la propia contratación de proveedores a través de vehículos jurídicamente válidos creados al efecto. Se trataba, pues, de un fondo de capital riesgo, pero descentralizado.

El 12 de junio de 2016, una vez puesto en marcha el proyecto, se detectó una brecha de base que podía ser utilizada por cualquiera de los que tuviera acceso a TheDAO para sacar no sólo su dinero, sino también el de los demás. A pesar de las declaraciones del líder del proyecto, Stephen Tual, de que no existía ningún riesgo y que los fondos estaban a salvo, el 17 de junio de 2016 comenzó el saqueo a TheDAO por parte de un «atacante», como él mismo se hizo llamar, que muy educadamente informó al resto de participantes de que su acción cumplía estrictamente con el contrato, no vulneraba el código y, por tanto, no violaba la ley. Hasta que el equipo del proyecto pudo frenarlo, moviendo los fondos que quedaban a una DAO hija,[113] el atacante sacó 60 millones de dólares. El atacante aprovechó un error de base del código, la función de split con la que se había construido la DAO, que le permitía sacar fondos (ajenos) sin que el balance de la DAO lo reflejase a tiempo. Así, conseguía sangrarla sin que el resto de participantes lo advirtiese.

Es de esperar que la experiencia de TheDAO sea valiosa desde un punto de vista técnico, pero no menos desde el jurídico y ético, ya que el robo en sí mismo constituía un acto criminal. La evolución de los Smart Contracts y los ICO definirán también el camino de futuro para las DAO desde un punto de vista legal.

Más información sobre cuestiones legales y jurídicas de la blockchain en <libroblockchain.com/legal/>.

SEGUNDA PARTE

La descentralización como modelo de vida

Capítulo 7

Hacktivismo, cypherpunks y el nacimiento de la blockchain

Cristina Carrascosa Cobos, Carlos Kuchkovsky Jiménez y Álex Preukschat

Hacktivismo, cyberpunks, cypherpunks y libertarismo, entre otros movimientos filosóficos y sociales similares del siglo XXI, se encuentran en el origen de la blockchain de Bitcoin. Todos ellos buscaban una nueva forma de relación en internet, así como una reinterpretación de conceptos como información, libertad y privacidad.

El papel de la criptografía

En su libro de 2001 *Cripto: cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital*, Steven Levy narra cómo la criptografía en Estados Unidos pasó en el plazo de cincuenta años de ser monopolio de la National Security Agency (NSA) a algo mucho más libre y diverso. Algunos de los protagonistas de ese proceso fueron Bailey Whitfield Diffie y Martin Hellman con el protocolo Diffie-Hellman; Ron Rivest, Adi Shamir y Leonard Adleman con el algoritmo RSA; Phil Zimmerman con PGP, o David Chaum con DigiCash. Son los inspiradores del movimiento de los cypherpunks que, influido por el hacktivismo y los cyberpunks, irrumpió con fuerza en la década de los noventa.

La protección de la privacidad y el uso de dinero anónimo son dos elementos esenciales tanto para entender el movimiento cypherpunk como la creación de Bitcoin. En fecha tan temprana como 1969, Bailey Whitfield Diffie ya dijo: «La criptografía es vital para la privacidad humana». Es decir, que en la era digital que entonces daba sus primeros pasos todo lo referido a ordenadores, correos electrónicos y comercio electrónico iba a necesitar de criptografía que protegiera las comunicaciones y la privacidad del conjunto de ciudadanos. El problema para Diffie empezó cuando advirtió que lo que se enseñaba en las

universidades era una criptografía muy básica y que las técnicas más avanzadas se hallaban en manos de la NSA. Lejos de desanimarse, decidió investigar más sobre el tema, prácticamente con la única ayuda de *The Code-Breakers*, un libro de criptografía de David Kahn que era entonces la única fuente disponible sobre la materia, pero tan valiosa que la propia NSA había intentado evitar su publicación en 1967.

La historia dio un giro decisivo cuando Diffie conoció a Hellman en Stanford y ambos unieron esfuerzos para crear mejores algoritmos criptográficos. Uno de los resultados de esa labor conjunta fue, en la década de los setenta, el concepto de criptografía de clave pública (Public Key Cryptography), esto es, el método criptográfico que se utiliza en comunicaciones electrónicas en internet vía SSL/TLS (lo que vemos como https mientras navegamos) y en criptomonedas como bitcoin. Poco después se les unió Ralph Merkle, el inventor de los Merkle Tree que se utilizan en la estructura de cadena de bloques de Bitcoin. Curiosamente, Diffie ya hablaba en aquellos años de «una visión descentralizada de la autoridad» que se acabaría haciendo realidad en Bitcoin.

DigiCash y el dinero digital

A finales de la década de los setenta, David Chaum decidió estudiar en Berkeley por la sencilla razón de que ahí se había formado Diffie. Chaum estaba interesado en protocolos de votación anónimos, los cuales le llevaron a la idea de crear dinero digital igualmente anónimo. En 1990, cuando la idea de que el dinero en papel iba a ser reemplazado por dinero digital se había convertido en algo generalmente aceptado, fundó DigiCash. Su tecnología se convirtió en algo ambicionado por compañías como VISA o Microsoft, que intentaron comprar sus patentes, pero sin alcanzar acuerdo alguno con Chaum. No obstante, la apuesta acabó fracasando y en 1998 DigiCash se declaró en quiebra. Uno de los errores que la condujeron a esa situación fue el de haber centrado sus esfuerzos en grandes corporaciones y entidades financieras en vez de en desarrollar una base de usuarios. Otro, el de emplear tecnología propia y protegida con patentes y licencias restrictivas, lo que hacía que las compañías usuarias de su solución tuviesen que confiar sus transacciones más sensibles en el buen o mal hacer de DigiCash y en un software que no podían revisar, mejorar o adaptar. Se trata de

errores que los que siguieron a esta iniciativa pionera han procurado no repetir. Así, Satoshi Nakamoto, el creador de Bitcoin, se centró en satisfacer la necesidad de los usuarios, sabedor que las empresas llegarían después.

Uno de los colaboradores de Chaum en DigiCash fue Zooko Wilcox-O'Hearn, el promotor y creador de la criptomoneda Z-Cash, que, desde su lanzamiento en 2016, pretende un anonimato garantizado de los tokens.

El origen del hacktivismo

En el documental *We are Legion*, estrenado en 2012, un hacker llamado Chris Wysopal afirma que L0pht y CdC eran dos colectivos de hackers que formaban parte de un todo: el primero se dedicaba a las actividades serias de inteligencia y seguridad, mientras que el segundo medía la longitud de un puente tomando como base a un amigo tumbado, entre otras acciones absurdas. Se trataba de las dos caras de una misma moneda: por un lado, la rama organizada, cuasi empresarial, que ansía la superación intelectual; por otro, la informal que simplemente disfruta haciendo cosas diferentes que estimulan su curiosidad e interés.

Fue en el seno de L0pht donde se pronunció por primera vez, de nuevo según Chris Wysopal, la palabra «hacktivismo». Con ella se quería definir un software destinado a facilitar la comunicación segura entre personas de distintos países y resistente incluso a aquellos Gobiernos que cayeran en la tentación de espiar a sus ciudadanos. El término se usaba también para invocar la libertad de expresión en las redes, la posibilidad de manifestarse y criticar al sistema establecido sin temor a represalias.

En la misma línea se pronunciaba Loyd Blankenship, alias *The Mentor*, cuando en 1986, bolígrafo en mano, redactó el manifiesto *La conciencia de un hacker* desde una celda en Estados Unidos. The Mentor estaba acusado de ser autor material e intelectual de una serie de delitos informáticos supuestamente cometidos a través de un grupo de juego de rol llamado GURPS Cyberpunk, y su condena incluía la prohibición de acercarse a un ordenador. Su relato es tanto un reproche a una sociedad que criminaliza al hacker sin detenerse a

comprender sus motivaciones, como una clara reivindicación de su acción: «Sí, soy un criminal. Mi crimen es la curiosidad». La esencia del hacktivismo ya está contenida en esas páginas.

Blankenship formaba parte de ese grupo de hackers que considera su «profesión» como algo digno, casi propio de un humanista por la unión que en ella se da de artesanía e inteligencia, y su rechazo de toda violencia. Los hackers se sienten entusiasmados por la creación y el desarrollo de las máquinas más sofisticadas y creen firmemente que la tecnología tiene el deber de «hacer algo», de aportar algo al mundo. Por ese motivo, comparten e intercambian ideas, códigos y consejos que utilizan para descubrir soluciones a problemas de tipo técnico.

El nacimiento de los cypherpunks

Otro grupo surgido entonces, el de los cyberpunks, tenía más de movimiento filosófico que tecnológico, no en balde tomó su nombre de un género literario y contracultural que estuvo en boga en la década de los ochenta. Idealmente, el cyberpunk es un individuo que defiende de forma exacerbada la libertad de expresión, la libertad de información y la privacidad de las comunicaciones. De los cyberpunks derivaron en 1992 los cypherpunks, que vieron en la criptografía y la tecnología el medio para alcanzar esos objetivos en el mundo digital. Su programa se halla recogido en *The Crypto-Anarchist Manifesto*, redactado en 1992 por el ingeniero estadounidense Tim May. Tanto este movimiento como la Electronic Frontier Foundation (EFF) se vieron inspirados por las ideas de Diffie, Chaum y Phil Zimmermann, el creador de PGP (Pretty Good Privacy), sin olvidar todo el legado del hacktivismo.

Además de aportaciones en el ámbito de la privacidad de las comunicaciones, el movimiento cypherpunk realizó varios experimentos de dinero digital. Entre ellos destacan los liderados por Wei Dai[114] y Nick Szabo, sobre todo porque en ellos (sin olvidar la tecnología desarrollada por DigiCash de David Chaum) encontró más tarde inspiración Satoshi Nakamoto para crear Bitcoin.

El hackeo de Netscape por los cypherpunk

A finales de la década de los noventa, quien más tarde sería el protagonista de la primera transacción de bitcoins con Satoshi Nakamoto, Hal Finney, propuso al grupo Cypherpunks@toad.com romper la versión internacional del navegador más popular de entonces, Netscape. Este software utilizaba la encriptación RC4 de 40-bit, a diferencia de la versión estadounidense, que era de 128-bit. La razón de esta diferencia se halla en las leyes de Estados Unidos, que no permitían a las empresas del país exportar productos con tecnología de cifrado «fuerte», comercio este sujeto a las mismas limitaciones que imperan para la exportación de armas.

El reto de Finney lo superó un estudiante llamado Damien Doligez, quien desde su casa en Francia consiguió romper la encriptación internacional de Netscape. La empresa achacó entonces la deficiencia en la seguridad a las leyes restrictivas de exportación que regían en Estados Unidos, abogando por un cambio en la normativa que evitara estos problemas. De este modo, los cyberpunks consiguieron su objetivo: denunciar a nivel internacional lo absurdo de las leyes promovidas por la NSA y el Gobierno de Washington, leyes que ponían en peligro el comercio electrónico y la competitividad de las empresas tanto estadounidenses como extranjeras.

Otro caso de activismo es el representado por Vitalik Buterin, uno de los creadores de Ethereum. En sus manifestaciones ha reconocido abiertamente que entre sus objetivos se encuentra materializar el sueño cypherpunk de otorgar todo el poder y control sobre sus datos y acciones al usuario. No obstante, el ejemplo más conocido de este movimiento por la repercusión que ha tenido a nivel mundial es Anonymous. Vendetta[115] lo describe perfectamente: Anonymous nace en 4chan[116] como algo casual, con un carácter más de broma que otra cosa. Los usuarios de la red propusieron entonces cambiarse todos el nick name a Anonymous para ver qué efecto hacía. Con el paso del tiempo y la sensación de comunidad que se creó en el foro, comenzaron a establecerse patrones de conducta y respuesta, además de una simbología propia que enlaza con las ideas de los cypherpunks.

Más información sobre el movimiento de los cypherpunks en la tecnología blockchain en <libroblockchain.com/cypherpunks/>.

Capítulo 8

La descentralización como modelo de vida

Álex Preukschat

A la hora de hablar del movimiento de la descentralización y de los principios filosóficos que hay tras él, el estadounidense Dee Hock, el fundador de Visa, es toda una referencia. Su libro *One From Many* teoriza sobre la organización caórdica, que fusiona el pensamiento sobre la estructura de las organizaciones y la esencia de la existencia de la vida, tal y como él la entiende. Por ello, cuando se hizo público que Hock se unía al consejo asesor de la startup Bitcoin Xapo,[117] Tommy Nicholas publicó un interesante análisis al respecto, titulado «Odd bedfellows: what a Bitcoin company can learn from the strange history of VISA».[118] Xapo es una de las empresas importantes del ecosistema de Bitcoin. Su director ejecutivo es Wences Casares, un argentino conocido por su férrea defensa del potencial de la tecnología de Bitcoin, aunque reconozca que las posibilidades de éxito de esta plataforma son todavía inciertas. De este modo, Dee Hock, el filósofo de la descentralización, y Wences Casares, el responsable de contagiar a muchos millonarios tecnológicos su pasión por Bitcoin, convergieron en una misma empresa para abordar temas clave como el de la blockchain pública.

Por qué el fundador de Visa se interesó por Bitcoin

En la historia de los negocios, Visa representa uno de los mejores ejemplos del exitoso empleo de la característica más vital de Bitcoin, la descentralización. Seguro que tú mismo o alguien de tu círculo más próximo ha usado alguna vez esa tarjeta de crédito o de débito para comprar o pagar algún servicio. Ahora bien, ¿podrías decir qué es lo que hace Visa? ¿Si mueve o no dinero? ¿Si fabrica las tarjetas de plástico o los terminales por los que pasa la tarjeta? En resumidas cuentas, ¿qué hace Visa, por qué y cómo? Sin duda, son preguntas interesantes y cuya respuesta el ciudadano de a pie habitualmente desconoce. Pues bien, Visa no fabrica ni vende tarjetas, no emite crédito, no mueve dinero, no construye ni vende terminales de pago ni realiza cualquier otra función de las que generalmente asociamos a las operaciones con tarjeta. En realidad, Visa no es

más que una red de telecomunicaciones que envía mensajes de pago por todo el mundo y garantiza que cada transacción que se aprueba será ejecutada. Eso es todo: una red de bits y una garantía para los bancos de que no se les defraudará.

En junio de 1970, y después de dos años trabajando en la reestructuración del BankAmericard, Hock se convirtió en director ejecutivo de una entidad independiente llamada National BankAmericard, que más tarde tomaría el nombre de Visa International. Desde esa posición puso las bases de lo que sería la popular tarjeta: una red descentralizada en la que miles de bancos y empresas individuales que compiten entre sí unen fuerzas para lograr un movimiento monetario a nivel mundial que beneficia a todos. Ciertamente, Visa se gestiona a través de una autoridad central, pero lo suficientemente descentralizada como para obtener dos de los principales beneficios de la descentralización: por un lado, la seguridad, tan necesaria para los bancos, de que los estándares se desarrollarán sólo bajo el interés superior de la red y no de una única entidad bancaria; por otro, la seguridad de que si cualquier banco socio de la red no cumple su obligación de liquidar una transacción, Visa cubrirá ese incumplimiento por defecto.

Paralelismos entre Bitcoin y Visa

Los paralelismos entre Bitcoin y Visa son numerosos, por lo que, tarde o temprano, debían coincidir. Bitcoin se fundamenta en la reducción total de la necesidad de la confianza, de tal modo que dos personas que no se conozcan de nada o desconfíen la una de la otra pueden llegar a ponerse de acuerdo en que «algo» es verdad. Para lograrlo, la compañía tiene una serie de mineros que garantizan la red, usuarios de su sistema y proveedores de servicios de empresas como Bitpay, Kraken, Coinbase o la mencionada Xapo. Cada uno de ellos facilita las transacciones digitales instantáneas en una red que funciona sin que nadie la observe, y sin que ninguna institución o proveedor pueda acabar con ella ni imponer su criterio al resto. Y todo porque la red se distribuye con protocolos que las partes no pueden cambiar.

Bitcoin, además, va un paso más allá porque funciona sin la necesidad de un punto central de confianza como el que representa Visa. De hecho, Bitcoin ni siquiera es una empresa: es un código abierto que cualquiera puede consultar,

contribuir o utilizar. Para Dee Hock, este valor añadido representa todo un avance cultural.

Bitcoin como cambio cultural hacia el mundo descentralizado

Para Dee Hock, en la actualidad estamos asistiendo al fin de una etapa de cuatrocientos años de edad y al nacimiento de otra nueva que comporta cambios mucho mayores que los habidos nunca en el mundo en la cultura, la ciencia, la sociedad y las instituciones. En su biografía *One From Many*, publicada en el año 2000, Hock explica cómo desde sus inicios profesionales quiso alejarse de «organizaciones jerárquicas que ejercen un fuerte control sobre todo y ahogan la creatividad e iniciativa desde las bases; un ambiente que convierte a la empresa en un ente demasiado rígido como para responder a los nuevos retos y oportunidades». Hock llegó a la conclusión de que el modelo de mando y control de la organización que se había instaurado para apoyar la revolución industrial se nos había ido de las manos. Simplemente no funcionaba, y ello porque trata a las personas como máquinas y hace que esas mismas personas, aunque individualmente se quejen de ese trato, caigan también en él cuando han de tratar con otros. Lo paradójico del caso es que esa robotización de los humanos convive con el intento de humanizar a las máquinas y hacer que se comporten como personas… Esta visión puede sonar ingenua, es cierto, y el mismo Hock es consciente de ello cuando reconoce que los conceptos de organizaciones caórdicas necesitan un siglo o más para madurar. Es como mirar un bebé e intentar imaginar su futuro: podemos tener una visión aproximada de lo que finalmente será, hombre o mujer, pero no del desarrollo de su ciclo vital.

Las personas no abandonarán los antiguos conceptos de organización por otros hasta que la propia inercia del movimiento arrastre a las masas hacia esas nuevas organizaciones, una vez se convenzan de que los resultados obtenidos con ellas son superiores. Tanto las blockchains públicas como las privadas pueden ser una muestra de ese mundo futuro que estamos dibujando. Más aun, son una invitación a experimentar el «caos» autorregulador de una organización que nadie controla completamente y en la que todos los que participan en ella son responsables de la misma. Al igual que sucede en el protocolo Bitcoin, donde la responsabilidad primera y prioritaria de cualquier nodo es la autogestión, también cualquier persona puede, con la autogestión, operar como

un buen nodo dentro de la red planetaria. De lo que se trata, pues, es de gestionar nuestra integridad, carácter, ética, conocimientos y comportamientos altruistas. Para Hock, sin conocernos a nosotros mismos es difícil que podamos gestionar, ayudar o apoyar a otros por las razones correctas.

El valor del autoconocimiento

Desde el núcleo duro de la tecnología global de Silicon Valley, muchas personas como Naval Ravikant (uno de los inversores de la criptomoneda Z-Cash y fundador de AngelList), Balaji Srinivasan (fundador y director ejecutivo de la startup Bitcoin 21 Inc) y Loic Le Meur (fundador de Le Web) insisten de forma recurrente en la importancia del autoconocimiento y la meditación, quizá conscientes de que todos nosotros somos nodos del planeta.

En España, esa idea de persona-nodo en comunión con los principios de la descentralización y la tecnología se halla presente en el yoga en escuelas como yoga naradeva que imparte la profesora Cristina Paz y en el *mindfulness* o conciencia plena que enseña Gustavo G. Diex y sus compañeros en el Instituto Nirakara de la Universidad Complutense.[119] Una de las muchas lecciones importantes que una y otro transmiten es que la condición básica para ser un buen nodo es amarse a uno mismo para luego poder amar y empatizar con el resto de personas (o nodos).

TERCERA PARTE

La tecnología blockchain

Capítulo 9

Criptografía y consenso aplicado a la blockchain

Jaime Núñez Miller

No es posible conocer el funcionamiento de la tecnología blockchain sin una aproximación a uno de sus elementos básicos, la criptografía. A partir de él se descubre todo su potencial en campos tan diversos de la vida como el industrial, el económico o el de la información.

La criptografía es el arte de transformar un mensaje legible en otro ilegible. A este proceso se le llama «cifrado», mientras que el contrario, la recomposición del mensaje en un formato legible, es el «descifrado». En la actualidad contamos con tres tipos principales de criptografía:

- Hashing.
- Criptografía simétrica o convencional.
- Criptografía asimétrica o de clave pública.

Los tres se usan de una u otra forma en el mundo de las criptodivisas o criptomonedas de las blockchains públicas y privadas.

El arte de «moler» contenidos

Hash es un verbo inglés que significa «picar» o «moler». Se trata de una expresión gráfica, pues la criptografía consiste precisamente en «moler» unos contenidos hasta obtener una secuencia de caracteres de una longitud fija, algo así como la huella digital de un mensaje o documento. En la práctica, el hash se obtiene aplicando una función matemática a unos datos. Siempre que apliquemos la misma función al mismo contenido, obtendremos el mismo hash. Del mismo modo, cualquier modificación del contenido, ya sea por corrupción o intervención intencional, cambiará por completo el hash resultante. Esto hace que las funciones hash tengan muchas aplicaciones en criptografía tanto para generar firmas digitales mediante algoritmos de autenticación como para

verificar la integridad de los datos en sistemas de *fingerprinting* (es decir, la identificación única e inequívoca de un dato, algo muy útil por ejemplo para encontrar archivos duplicados).

El hash se obtiene aplicando, valga la redundancia, una función hash, a veces también llamada «resumen» o *digest*, que arrojará un resultado similar al que vemos en los siguientes ejemplos:

Mensaje	Resultado hash (hexadecimal)
«Perro»	5CDC4F3FEB31CEB78
«El perro de San Roque»	96C32852CB4C69E71
«El perro de San Roque»	20B003E7747353A6F

El propósito de un hash no es el de ocultar el mensaje en sí, ni el de permitir descifrarlo después, sino el de comprobar su integridad y verificar que no ha sido alterado. Los editores de software, por ejemplo, publican archivos junto con su correspondiente hash, de modo que los usuarios que se los descargan pueden luego calcular el hash de cada uno de ellos y compararlo con el que publicó el editor. Si los hashes son idénticos, los usuarios saben que los archivos no se han alterado o corrompido por el camino. Todo esto que parece tan técnico es fundamental en la minería de bitcoins u otras criptomonedas que utilizan sistemas de Prueba de Trabajo (Proof of Work, en inglés, PoW), y así lo veremos cuando hablemos de la capacidad de hasheado de una red, concepto importante para todas las aplicaciones de la tecnología blockchain.

Las funciones hash, un ejemplo de funciones unidireccionales

Una función unidireccional es una función matemática que funciona, como su nombre indica, en un solo sentido. Es decir, que una de las partes conoce un procedimiento de cálculo eficiente y rápido para computar esa función, mientras que la otra lo desconoce, por lo que le resulta prácticamente imposible realizar ese mismo cálculo a la inversa en un tiempo razonable. Un ejemplo de este tipo de función consiste en la factorización de números enteros: multiplicar dos números primos grandes de centenas o miles de bits es viable y fácil para los ordenadores actuales; sin embargo, no se conoce un algoritmo eficiente para invertir esta multiplicación, es decir, recuperar los dos primos iniciales partiendo exclusivamente de su producto.

Las funciones se distinguen entre sí por sus características fundamentales:

- **Eficiencia de cálculo:** que se pueda generar rápidamente y a bajo coste.
- **Resistencia a preimagen:** que sea computacionalmente muy difícil obtener un mensaje de entrada que produzca un hash predeterminado; es decir, que no se pueda prever el hash que se va a generar con un mensaje de entrada.
- **Resistencia a segunda preimagen y a la colisión:** que sea computacionalmente muy difícil crear dos mensajes distintos que den como resultado el mismo hash.

Las funciones hash forman parte de estas funciones unidireccionales. Teóricamente, y dado que el tamaño del hash es generalmente más reducido que el mensaje de entrada, podrían existir varias entradas diferentes que darían el mismo hash. Es lo que se llama colisión, si bien las buenas funciones hash hacen que algo así sea prácticamente imposible.

Con el avance de la tecnología, el diseño de funciones hash se ha ido mejorando gracias a las pruebas de ataque realizadas por los criptoanalistas. Por ejemplo, los algoritmos de funciones hash desarrolladas y utilizadas en la década de los noventa, como MD5 o SHA-1, en la actualidad o están rotos o significativamente amenazados. Ello hace que Bitcoin utilice dos tipos de algoritmos de hash: SHA-256, como función hash principal, y RIPEMD-160, en el proceso de creación de direcciones. En la realidad práctica de cada blockchain pública o privada, la combinación de las tecnologías de criptografía depende de las decisiones que tomen los desarrolladores.

El primero de esos algoritmos, SHA-256 (SHA significa *Secure Hash Algorithm*, en inglés), pertenece a la familia de funciones de hash SHA-2 diseñadas por la National Security Agency (NSA) o Agencia de Seguridad Nacional, encargada de todo lo relacionado con la seguridad de la información en Estados Unidos. Estas funciones son aceptadas por el National Institute of Standards and Technology (NIST) como el estándar en algoritmos de hash para la administración estadounidense. Sustituye a su predecesor el SHA-1.

En cuanto a RIPEMD-160 (RIPEMD significa *RACE Integrity Primitives Evaluation Message Digest*, en inglés), se utiliza en el protocolo Bitcoin cuando se requiere un hash de menor longitud. Fue creado en 1996 y pertenece a la

familia RIPEMD que dispone de longitudes de salida de 128, 160, 256 y 320 bits. Bitcoin usa la versión de 160 bits.

Doble hash para garantizar la seguridad contra el criptoanálisis

Para garantizar la seguridad, en el protocolo Bitcoin los hashes son el resultado de aplicar dos veces un algoritmo de hash. Vamos a verlo con un ejemplo:

SHA-256(SHA-256 («perro»))

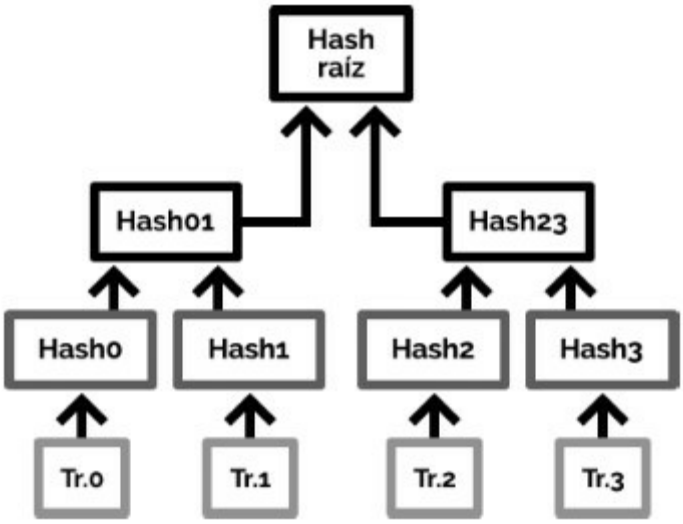
El resultado final sería el hash SHA-256 del hash SHA-256 del texto «perro».

2efe5fccbc3639fe5fd4582926c84d2e456a58033096cc1d554701d3474f9

Los hashes se utilizan en el protocolo Bitcoin con diferentes propósitos. Por ejemplo, todas las transacciones de bitcoins son mensajes cuyo hash se utiliza para identificarlas de forma única. El TXID (Transaction ID), que identifica cada transacción de forma inequívoca, es el resultado de aplicar una doble función SHA-256 como la del ejemplo de arriba a la transacción enviada a la red.

En 1979, el criptógrafo Ralph Merkle inventó un hash al que dio su nombre, el *Merkle Tree* o «árbol de Merkle». Se trata de una formación piramidal de hashes en la que cada hash es el resultado de aplicar una función de hash sobre los hashes inferiores hasta llegar al nodo raíz o *Merkle Root* del árbol en cuestión. Estos árboles de Merkle permiten verificar de forma eficiente y segura la integridad y la inclusión de grandes cantidades de datos. El protocolo Bitcoin y otros protocolos de criptomonedas y blockchains privadas utilizan los Merkle Trees en la cadena de bloques. La cabecera de cada bloque contiene entre otros datos el nodo raíz (*Root Hash*) de todas las transacciones incluidas en el bloque.

Modelo de Merkle Tree o árbol de hash.



Criptografía simétrica o convencional

La criptografía simétrica utiliza una sola clave tanto para cifrar un mensaje como para descifrarlo. En los primeros tiempos de esta disciplina, la seguridad de los mensajes cifrados se basaba en el uso de algoritmos secretos. El problema era que cualquiera que conociera su clave podía descifrarlos. En la actualidad, los algoritmos más usados son de dominio público y conocidos por todos, por lo que la seguridad se basa en una clave y sólo aquellos que la conocen pueden descifrar el mensaje.

Claves y contraseñas

Una clave y una contraseña no son lo mismo. Las primeras son más seguras que las segundas por su gran tamaño y porque se suelen generar de forma aleatoria. Las contraseñas, en cambio, son más cortas y están pensadas para que una persona las pueda memorizar, lo que las hace más vulnerables. Como las claves no se pueden recordar, muchas veces se guardan en archivos que se cifran y descifran mediante una contraseña, lo que no deja de ser paradójico: es como guardar dentro de un cajón cerrado con una llave común una llave de alta seguridad que lleve a una cámara acorazada. La forma más segura de generar y guardar claves privadas es mediante dispositivos hardware específicamente creados para ello. En el ecosistema Bitcoin, por ejemplo, existen dispositivos conocidos como *hardware wallets*.

El reto en la criptografía de una sola clave es encontrar una forma segura de entregar ésta al destinatario para que pueda descifrar el mensaje. Pero si ya existe una forma segura para entregar la clave, ¿por qué no utilizarla también para enviar el mensaje? La respuesta es que la criptografía simétrica es más eficiente cuando no se requiere enviar la clave a otra persona. Un ejemplo lo vemos al cifrar un archivo en el propio disco duro, usando la misma clave para cifrarlo y descifrarlo.

Uno de los algoritmos más conocidos para el cifrado con clave simétrica es AES (Advanced Encryption Standard) que utiliza claves de hasta 256 bits, o lo que es lo mismo 2^{256} combinaciones posibles de ceros y unos. Es el mismo tamaño que usan las claves ECDSA de Bitcoin y consisten en 256 posiciones compuestas de ceros y unos en una secuencia aleatoria. Un ejemplo:

0111010100101011101011110100101011010010000101101010100100111010111110100010100101

Para hacernos una idea de la cantidad de combinaciones posibles que ofrece una clave de 256 bits, basta con saber que se tiene que representar con una cifra decimal de 77 cifras de largo. La clave de arriba en formato decimal sería el impronunciable número:

52.997.787.530.799.283.151.858.736.196.373.174.009.060.844.085.335.115.422.872.086.384.222.9

El tamaño de la clave es uno de los datos críticos para determinar la seguridad del cifrado frente a ataques de fuerza bruta. Cuanto mayor sea el número de claves posibles, más difícil será para una computadora encontrar la clave válida. Por ejemplo, para recorrer la mitad de las claves disponibles en AES256, sin hacer ningún cálculo adicional, deberíamos dedicar 150 centrales nucleares que proporcionen energía constante a las 10^{38} supercomputadoras *Tianhe-2* que serían necesarias durante un tiempo equivalente a la actual edad del universo. Este tamaño de claves es resistente en la práctica incluso a los posibles ataques mediante computación cuántica.

Criptografía asimétrica o de clave pública

La criptografía asimétrica utiliza dos claves, una pública y otra privada, ambas creadas y vinculadas entre sí mediante una función especial. Esas funciones calculan la clave pública a partir de una clave original (clave privada) que se genera de forma aleatoria.

La clave privada la guardamos en secreto y la pública la podrá conocer todo el mundo. Con esa clave pública cualquiera podrá cifrar los mensajes secretos que nos quieran enviar y sólo nosotros los podremos descifrar con nuestra clave privada. El detalle interesante aquí es que la clave con la que se cifra un mensaje no sirve para descifrarlo. Tendremos que usar la otra clave para descifrar los mensajes.

Un ejemplo: Alicia envía un mensaje cifrado a Bob:

En este ejemplo, si Alicia quiere enviar un secreto a Bob, sólo tiene que buscar y verificar la clave pública de Bob, cifrar el mensaje con esa clave y enviárselo a Bob. Cuando Bob reciba el mensaje usará su clave privada para descifrarlo.

Si conocemos la clave privada, podremos averiguar cuál es su clave pública, pero no al revés; es decir, si conocemos la clave pública no podremos obtener la privada. Las funciones de clave asimétrica son otro ejemplo de funciones unidireccionales o funciones trampa de un solo sentido.

La clave privada no es más que un número aleatorio tan grande que hace que probabilísticamente resulte imposible generar otra igual. A partir de ella se calcula la clave pública usando un algoritmo como por ejemplo RSA o ECDSA. Este último (Elliptic Curve Digital Signature Algorithm) es el usado por Bitcoin.

La clave privada en el contexto de Bitcoin es un número aleatorio de 256 bits (256 ceros y unos) que se suelen representar en sistema hexadecimal (en caracteres del 0 al 9 y de la A a la F). Un ejemplo de clave privada es éste:

E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6
1F 20 BD 67 FC 23 3A A3 32 62

Esta clave es la única que nos permitirá mover los bitcoins vinculados a ella. Las claves privadas se generan y se guardan en un *wallet* o cartera Bitcoin.

El sistema hexadecimal

Ese ejemplo de clave en el contexto de Bitcoin sigue un sistema de numeración adecuado para las computadoras y que tiene como base el número 16 (sistema hexadecimal), en vez del 10 (sistema decimal) que usamos habitualmente. Los caracteres que se usan para representar esos 16 números básicos son: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. En él, cada pareja de caracteres, por ejemplo E9, representa un *byte*, que es la unidad mínima de memoria en computación y que consiste en una secuencia de ocho ceros y unos. Todas las parejas posibles (16 × 16) nos permiten representar hasta 256 posiciones decimales o lo que es lo mismo, el total de combinaciones posibles de ocho ceros y unos. Veamos algunos ejemplos:

Binario	Hexadecimal	Decimal
00000000	00	0
00000001	01	1
00001000	08	8
10000000	80	128
10000001	81	129
11111111	FF	255

Volviendo a la clave de Bitcoin que empezaba con el byte E9, sería:

Hexadecimal	Decimal	Binario
E	14	1110
9	9	1001

Eso quiere decir que nuestra clave privada en realidad empieza con el byte 11101001 y que por comodidad y legibilidad lo escribimos en su forma hexadecimal E9. Para avisar que una cifra está expresada en su forma hexadecimal se añade en muchas ocasiones el prefijo 0x. Por ejemplo, 0xE9 sería el inicio de nuestra clave privada (E9...).

ECDSA (Elliptic Curve Digital Secure Algorithm) para crear claves privadas y públicas

La criptografía de curva elíptica (Elyptic Curve Crytpgraphy, ECC) es una de las formas que permiten obtener una clave pública y una de las tecnologías criptográficas más prometedoras. Proporciona la misma o mayor seguridad que

el resto de algoritmos de clave pública, pero es más eficiente, rápida y escalable. Se utiliza en las blockchains para obtener las claves públicas y firmar/verificar las transacciones.

No obstante, el algoritmo de clave pública más conocido es el RSA, que muy resumidamente consiste en multiplicar dos números primos. Como ya vimos antes, se trata de una función unidireccional, es decir, muy fácil de calcular en un sentido, pero muy difícil de hacerlo en el contrario. De una forma extremadamente básica, su principio funciona así: pongamos que nos dieran estas combinaciones de números 456, 645, 835, 2345 y multiplicásemos sus cifras entre sí. Los resultados podrían ser algo parecido a esto:

$$4 \times 5 \times 6 = 120 \quad 6 \times 4 \times 5 = 120 \quad 8 \times 3 \times 5 = 120 \quad 2 \times 3 \times 4 \times 5 = 120$$

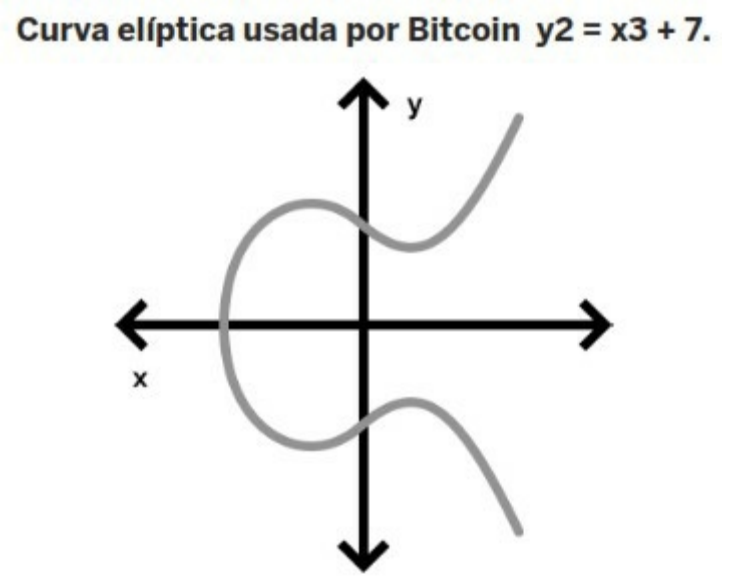
Todos darían la misma cifra, 120. Sin embargo, si nos dieran el número 120 (clave pública) no se podría saber con seguridad qué combinación inicial (clave privada) hemos utilizado para llegar a 120, porque todas arrojan el mismo resultado.

Si elevamos la complejidad de este principio de irreversibilidad o unidireccionalidad utilizando grandes números primos, seguiría siendo fácil hacer la multiplicación, pero enormemente difícil obtener los números originales (clave privada) factorizando el resultado (clave pública) y especialmente si utilizamos números primos. Los números primos tienen propiedades especiales que los hacen muy valiosos en las funciones criptográficas. Cuando Rivest, Shamir y Adleman (RSA) propusieron su criptosistema a mediados de la década de los setenta, seguramente no imaginaban la importancia que llegaría a tener su invención para crear sistemas seguros en internet.

Los algoritmos de curva elíptica ECC, tanto ECDH (Elliptic Curve Diffie-Hellman) que se usan para cifrar, como ECDSA, no utilizan números primos, sino coordenadas en una curva elíptica. En su representación algebraica, una curva elíptica se expresa con la siguiente ecuación:

$$y^2 = x^3 + ax + b$$

Dependiendo del valor de a y b, las curvas elípticas tomarán distintas formas en el plano. En el caso de Bitcoin, se utiliza una curva elíptica ECDSA en la que a = 0 y b = 7 y se suele representar así:



Una de las ventajas de los sistemas de curva elíptica (ECC) es que requieren números de tamaños menores que RSA para proporcionar el mismo nivel de seguridad. Una clave ECC puede ser diez veces menor (consume menos memoria) y el algoritmo es bastante más rápido de procesar en la mayor parte de las operaciones. Éste es el principal motivo por el cual Satoshi Nakamoto optó por el estándar de curva elíptica ECDSA para el protocolo Bitcoin.

Bitcoin utiliza la aritmética de las curvas elípticas para obtener claves públicas, firmar las transacciones y verificar esas firmas. Los conceptos matemáticos requeridos para entender el proceso en detalle son bastante complejos, algo lógico si se tiene en cuenta que la parte criptográfica es fundamental en todas las criptodivisas y sistemas blockchain. Una explicación más detallada de estos conceptos se encuentra en <libroblockchain.com/ecdsa/>.

¿Son seguros en el tiempo los algoritmos de clave pública?

Con la tecnología actual no se conoce ninguna forma de obtener una clave privada a partir de su clave pública, pero eso podría cambiar en el futuro. Ninguna función de clave pública, ya sea RSA, DSA, DH y ECC, puede garantizar su seguridad en los años venideros, entre otras cosas porque es

imposible saber cómo van a evolucionar los sistemas de criptoanálisis, las computadoras cuánticas y los algoritmos para factorizar grandes números. En el actual protocolo Bitcoin sólo se revelan las claves públicas cuando se realiza una transacción. Si nuestras criptomonedas permanecen quietas en una dirección no se conocerá su clave pública y no se podrá ni siquiera iniciar el ataque para encontrar la clave privada:

- La «clave privada» siempre es secreta.
- La «clave pública» es secreta hasta que se hace una transacción.
- La «dirección» (el hash de la clave pública) siempre es pública.

El proceso para generar una nueva dirección Bitcoin no requiere una autoridad central, simplemente parte de una clave privada (número aleatorio) a la que se le aplican los siguientes algoritmos:

Cuando hablamos de atacar el sistema nos referimos a encontrar la clave privada, que es la única que nos permite firmar una transacción y, por tanto, cambiar la titularidad de unas criptomonedas. Si se llegaran a inventar computadoras y algoritmos capaces de revertir la criptografía de curva elíptica, nuestras criptomonedas sí estarían en peligro durante el momento en el que se tramita la transacción. Eso ocurre porque al realizar una transacción tenemos que revelar obligatoriamente la clave pública de las criptomonedas que queremos mover. Entonces y hasta que la transacción no esté confirmada, se

podría iniciar un ataque tomando como dato la clave pública. Recordemos que eso no es posible en la actualidad, pero si algún día se llegara a sospechar que sí fuera posible, deberíamos dejar de hacer transacciones hasta que se solucionara el problema.

La segunda forma de protección se refiere a los protocolos blockchain, que pueden actualizarse y cambiar su algoritmo de clave pública para utilizar uno más resistente. Para ello sería necesario contar con ese algoritmo y aceptar un cambio vía *hard fork* (un cambio irreversible en el protocolo, no compatible con versiones anteriores).

El problema de los generales bizantinos y su importancia en la blockchain

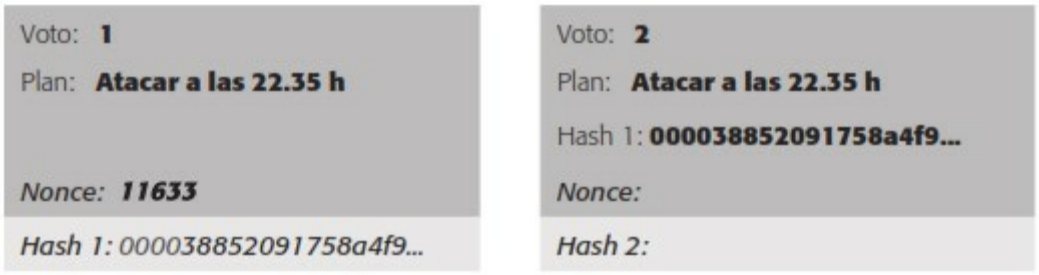
La demostración que representa Bitcoin de que se puede alcanzar un consenso descentralizado al margen de cualquier tipo de autoridad central ha abierto todo un horizonte de posibilidades en los terrenos más diversos. La criptografía, las matemáticas, la teoría de juegos e internet son los cimientos de esta ciencia que ya ha dejado las pizarras para empezar a cambiar el mundo real. Hace tiempo que las ciencias de la computación estudian fórmulas para lograr que un sistema descentralizado pueda sincronizarse evitando los fallos y posibles ataques en redes abiertas. Para entender exactamente toda esta cuestión recurriremos a un dilema clásico en seguridad para sistemas descentralizados conocido como el «problema de los generales bizantinos». Se le llama así porque en su formulación típica plantea el caso de un grupo de generales de ese antiguo imperio que están dispersos y que deben ponerse de acuerdo en atacar una ciudad o en retirarse. El plan sólo tendrá éxito si la mayoría ataca al mismo tiempo o se retira, pero sólo se pueden comunicar entre ellos mediante mensajes. No hay ninguna autoridad que los coordine e incluso podría darse el caso que alguno de ellos fuera un traidor e intente sabotear el consenso. Hasta que Satoshi Nakamoto no publicó el protocolo Bitcoin no se conocía ninguna solución práctica a este problema. La propuesta de Satoshi hace uso de un sistema inventado en 1997 por el criptógrafo inglés Adam Back, llamado *hashcash*, que explicamos en más detalle en <libroblockchain.com/hashcash/>.

¿Cómo resolvió Satoshi el dilema? Pues de manera tan simple como creando una cadena de pruebas de trabajo. Vamos a intentar visualizarlo.

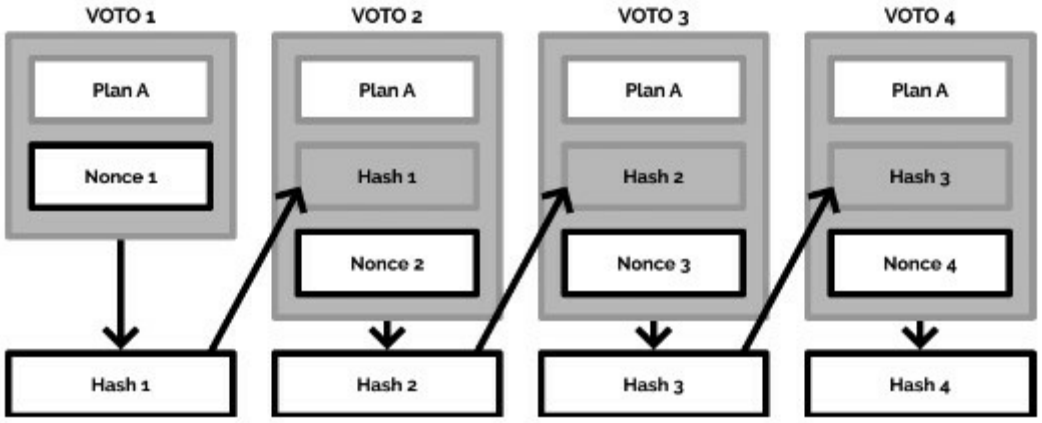
Supongamos que hay cuatro generales y que cada uno de ellos tiene un ordenador capaz de recibir y enviar mensajes, y de calcular hashes. Se ha decidido que cualquier general puede proponer la hora para el ataque, que llamaremos «el Plan», y cualquier plan que se envíe primero deberá ser el Plan oficial que seguir. El problema es que la red no es instantánea, puede haber cortes, etc., y si dos generales anuncian diferentes planes al mismo tiempo, algunos pueden recibir antes el Plan A y otros el Plan B, sin que puedan saber cuál de ellos fue el primero. Se necesita, por tanto, un sistema para llegar a un acuerdo sobre el Plan que ejecutar. Para solucionar eso utilizaremos una blockchain, a la que también podríamos llamar «cadena de pruebas de trabajo» o, más acorde con este caso, «cadena de votos». Los generales irán añadiendo sus votos a una cadena que representa un plan, de tal modo que si hubiera dos planes, entonces tendrían dos cadenas y deberán decidir a cuál de ellas votar. Todos ellos tienen una copia de ambas cadenas.

El derecho a emitir un voto lo obtienen de la siguiente forma: cuando un general decida comunicar a los demás su plan por primera vez, pondrá su ordenador a buscar un hash de una dificultad predeterminada, tal y como se hacía con *hashcash*. Esta vez el mensaje a hashear es el Plan (por ejemplo, «Atacar a las 22.35 h») y se ha establecido que la dificultad del hash, para que sea aceptado por los demás, tenga al menos cuatro ceros delante. También se ha previsto que, sumando la potencia de sus ordenadores, alguno de los cuatro generales llegará a encontrar un hash de esa dificultad en un plazo aproximado de 10 minutos. Eso quiere decir que entre todos se podrá crear un voto cada 10 minutos. Otra de las reglas consensuadas con anterioridad es que el plan que más votos tenga al cabo de dos horas será el plan que ejecutar. En ese tiempo ya habría unos doce votos y si el ordenador entregado a cada uno tiene la misma potencia, la probabilidad de encontrar un hash (el derecho a un voto) será igual para todos y, por tanto, la media sería de tres votos por cabeza en ese plazo de dos horas. La mayoría habrá podido votar y conocerá el plan.

Cuando un general logre enviar un plan con su hash correcto, ése será el primer voto válido y el primer eslabón de esa cadena. Enviará a todos los demás el número de voto, el plan, el nonce (al igual que en el protocolo *hashcash*) y el hash. Seguidamente, todos ellos empezarán a buscar el segundo hash usando además el hash anterior como parte del contenido a hashear.



El general que encuentre el siguiente hash (el segundo voto de la cadena) se lo enviará a los demás para que alguno de ellos logre crear el tercer voto, y así sucesivamente. Cada vez que un general encuentra y publica el hash, está emitiendo un voto por el plan que contiene esa cadena.



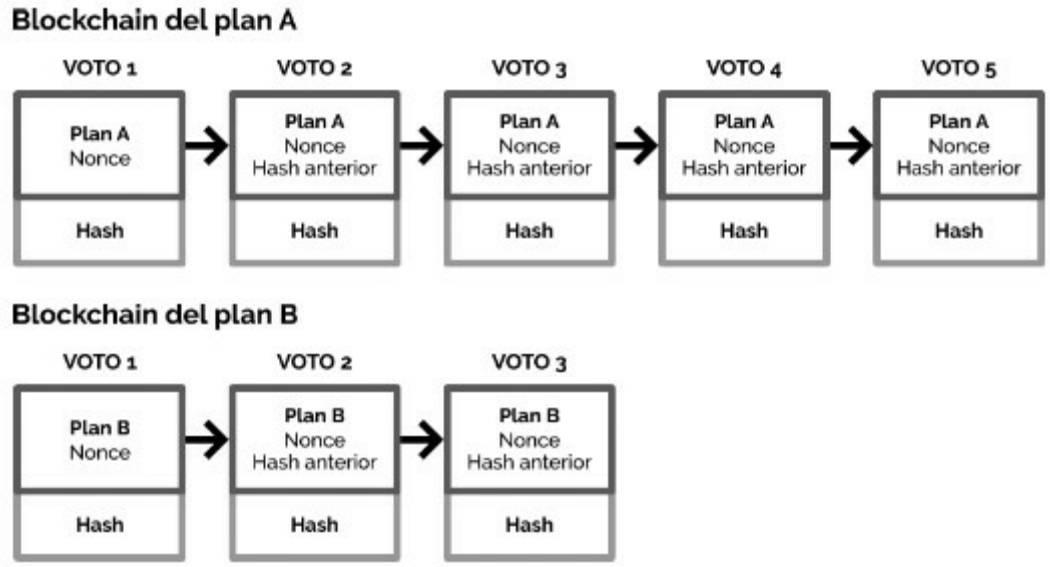
En poco tiempo se empezará a formar una cadena de hashes o pruebas de trabajo enlazadas entre sí. Pero ¿para qué se necesita una cadena? En esencia para llevar la contabilidad de los votos y que se puedan verificar independientemente por cada uno de los generales. Cada vez que reciben un nuevo voto y antes de sumarlo a su copia de la cadena, realizarán las siguientes comprobaciones:

1. ¿Comienza con cuatro ceros el hash del nuevo voto?
2. ¿Se obtiene ese hash con los contenidos hash (número de voto + el plan + hash del voto anterior + nonce)?
3. ¿Es el mismo plan que el del voto anterior?

Cada general puede verificar esos datos e ir añadiendo los votos recibidos a su copia de la cadena.

Dos cadenas

Si alguno de los generales hubiera publicado otro plan de forma simultánea al primero, los generales podrían llegar a tener dos cadenas distintas, cada una con un plan diferente. En ese caso necesitan elegir a qué plan votar y lo harán ignorando aleatoriamente una de las dos cadenas. A medida que se vayan emitiendo votos una de las dos cadenas tendrá ya una ventaja palpable sobre la otra.



Como a la mayoría les interesa llegar a un acuerdo, ignorarán el plan con menos votos y seguirán votando al que ya más votos tenga acumulados. Recordemos que les da igual a qué hora atacar, lo importante es que estén de acuerdo en un mismo plan y así garantizar el éxito del ataque. Como veremos más adelante en el capítulo que explica el funcionamiento de la blockchain, la existencia de un incentivo es vital para mantener el consenso. En el caso de Bitcoin consiste en lograr los nuevos bitcoins y comisiones que se generan con cada bloque. Finalmente para nuestros generales, la cadena más larga, la que haya acumulado más pruebas de trabajo (más votos) en esas dos horas, será el plan acordado. Ahora ya podrán atacar sabiendo que la mayoría de generales apoya el mismo plan.

La resolución del dilema sirvió para solventar un problema que hasta entonces había parecido irresoluble: el del doble gasto en un sistema descentralizado. Al tratarse de sistemas descentralizados, hace falta un método para llegar a un acuerdo (como en el caso de los generales bizantinos) respecto al orden en el que se registran las transacciones. Este método, en el caso de Bitcoin, se llama Cadena de Prueba de Trabajo (Proof of Work Blockchain, en

inglés). El blockchain es un registro cronológico de transacciones consensuado por todos sus usuarios y por tanto se puede usar para evitar el doble gasto, es decir, para impedir que alguien transfiera dos veces el mismo token. Las blockchains registran cada transacción en orden de aparición. Si Manuel le manda un token a Alicia, no podrá más tarde enviarle el mismo token a Bob.

La innovación más importante que nos ofrece la tecnología blockchain consiste precisamente en ese mecanismo que nos permite alcanzar un consenso entre partes que no se conocen a través de una red pública y potencialmente comprometida. En el capítulo de la transacción Bitcoin veremos cómo Satoshi Nakamoto mejoró este mecanismo y los detalles de cómo se aplica para construir una blockchain. No obstante, para explicar en detalle cómo se alcanza el consenso en Bitcoin haría falta un libro entero. Por eso, recomendamos completar la presente lectura en <libroblockchain.com/consenso/>.

Capítulo 10

Software libre y código abierto en el mundo de las blockchains

Víctor Escudero Rubio

El concepto de código abierto es otro de los aspectos importantes que hay que conocer para entender la dinámica de mercado de la tecnología blockchain. Su aplicación en el mundo de las blockchains públicas y privadas no es igual y no todo lo que se llama software de código abierto es software libre. Éste es aquel que permite a los usuarios utilizar, estudiar, mejorar y/o redistribuir el mismo, bien en su forma original o con las modificaciones que se realicen con posterioridad. Para estudiar un software, para mejorarlo o adaptarlo a las necesidades de cada uno, es imprescindible disponer del código fuente. Sin embargo, no debemos confundir software libre con el software de código abierto. El software libre requiere obviamente disponer de código abierto, si bien lo contrario no es siempre cierto. Existen numerosas licencias de código que, aunque aseguran la disponibilidad del código fuente, impiden su modificación o su uso con determinados fines, por ejemplo, comerciales o militares.

Cuando se otorga acceso al código fuente y se permite su modificación, la comunidad de programadores puede realizar sus aportaciones para solucionar eventuales fallos, incrementar la usabilidad o mejorar el programa a nivel general, lo que deriva normalmente en un programa de mayor calidad. Este proceso, al tener una naturaleza descentralizada es, a menudo, más complejo que en sus homólogos de código propietario, donde el control reside en manos de unos pocos desarrolladores que trabajan bajo las directrices de una misma organización.

Las cuatro libertades básicas que otorga el software libre —libertad para usar, estudiar, mejorar y distribuir el software— se pueden desglosar en mayor medida en los siguientes requisitos:

- Libre distribución.

- El código fuente debe estar incluido u obtenerse libremente.
- La redistribución de modificaciones debe estar permitida.
- Integridad del código fuente del autor: las licencias pueden requerir que las modificaciones sean redistribuidas sólo como parches.
- Sin discriminación de personas o grupos para su uso.
- Sin discriminación de áreas de iniciativa, incluso las comerciales.
- Distribución de la licencia: deben aplicarse los mismos derechos a todo el que reciba el programa.
- La licencia no debe ser específica de un producto: el programa no puede licenciarse sólo como parte de una distribución mayor.
- La licencia no debe restringir otro software: no puede obligar a que algún otro software que sea distribuido con el software abierto deba ser también de código abierto.
- La licencia debe ser tecnológicamente neutral.

El organismo que vela por el reconocimiento del software libre y que en gran medida determina los límites de lo que se considera software libre frente a software de código abierto se denomina OSI (Open Source Initiative).[120]

El software libre del protocolo Bitcoin

GNU/Linux, Android, Apache, LibreOffice, el navegador de internet Firefox de Mozilla o el antivirus ClamWin son algunos ejemplos de código abierto. Otro es el protocolo Bitcoin y muchas de las blockchains públicas. El protocolo Bitcoin y su software se publican abiertamente y cualquier programador en cualquier lugar del mundo puede revisarlo o crear su propia versión modificada. Bitcoin tampoco tiene propietarios, sino que lo controlan los usuarios que tiene en el mundo, sus mineros, desarrolladores y, en fin, todos aquellos que participan de ese ecosistema, una situación esta que dificulta forzar cambios en su protocolo, pues los participantes son libres de elegir el software y la versión que quieran. Eso sí, para que sigan siendo compatibles entre sí, todos los usuarios necesitan utilizar software que cumpla con las mismas reglas. Esto hace que exista un delicado equilibrio dinámico entre las fuerzas que ejercen los desarrolladores

cuando introducen nuevas funcionalidades al protocolo, el uso que de él hagan los usuarios y los incentivos que puedan tener los mineros para empezar a utilizarlo.

Desde el principio, la idea de Bitcoin resultó tan disruptiva, que fue rechazada de plano incluso por muchos de los mismos usuarios que más tarde terminarían por rendirse a ella. La solución parecía tan «simple» que, una vez desvelada, parecía imposible que a nadie se le hubiese ocurrido antes resolver el problema del doble gasto, por lo que rápidamente se empezó a escrutar el whitepaper y el código fuente de la implementación de referencia de Bitcoin en busca de puertas traseras. Pero, sorprendentemente, esta primera blockchain resultó ser más sólida de lo que sus detractores esperaban. Sin una documentación de referencia clara y transparente del funcionamiento de esta primera blockchain y sin acceso al código fuente para poder investigar sobre la nueva tecnología, difícilmente ésta hubiese podido despegar.

La bifurcación del protocolo Ethereum durante el verano del año 2016 (la tercera hasta esa fecha) constituye otro ejemplo interesante en el que la comunidad de una blockchain pública no llegó a ponerse de acuerdo sobre la evolución del protocolo, creando una bifurcación en el recorrido de la cadena de bloques que se adueñó del nombre de Ethereum y que dejó de ser compatible con la versión histórica, la cual siguió con el mismo funcionamiento y se llamó Ethereum Classic, tal como se explica en el capítulo de inversión en criptomonedas.

Bitcoin sólo puede funcionar correctamente si hay consenso entre todas las partes y es precisamente ahí donde radica gran parte de su fortaleza y su debilidad. Por lo tanto, todos los usuarios, mineros, inversores y programadores comparten un gran aliciente para proteger dicho consenso. Un aspecto interesante es que cualquiera puede copiar y utilizar el código del protocolo Bitcoin como quiera, pero si no cuenta con un apoyo significativo de la comunidad no tendrá éxito en el medio-largo plazo.

El código fuente de Bitcoin ha sido utilizado como la base para muchos otros proyectos de software. La forma más común de software generado a partir de él son otras criptomonedas o tokens.

La licencia de protocolo Bitcoin es MIT License

La MIT License es la licencia de software elegida en su día por Satoshi Nakamoto para Bitcoin. Se trata de una licencia que, al igual que otras muchas como BSD, suele ser utilizada cuando el creador del software quiere que el código sea accesible para el mayor número de desarrolladores y trabajos derivados posibles. Además, no importa lo más mínimo dónde o cómo vaya a ser el futuro uso del código, ya que éste puede reescribirse bajo una licencia del tipo que sea, incluso privativa. Es, por lo tanto, una licencia de código abierto (*open source*), libre (*free software*) y sin copyleft, es decir, es completamente permisiva y sin protección heredada. Técnicamente se trata de una licencia corta, sencilla y fácil de entender.

Las blockchains privadas de código abierto

Muchas de las iniciativas relacionadas con el mundo de las blockchains privadas se sustentan también en desarrollos de código abierto, lo cual no es casualidad. R3 (R3CEV LLC) es un claro ejemplo de compañía formada por un consorcio de más de setenta bancos e instituciones financieras que, haciendo uso de la infraestructura de una blockchain pública como Ethereum, implementó su propia cadena de bloques privada. Posteriormente creó internamente su propia plataforma, llamada Corda, para más tarde terminar liberándola como código libre. Otras iniciativas nacidas del ámbito privado, como Ripple, han recorrido un camino similar hasta desembocar en licencias de código abierto para garantizar su propia supervivencia.

Todas las cadenas de bloques han de lidiar con el problema de la falta de confianza entre las partes. Pero el problema se vuelve mucho más acuciante en el caso de las blockchains privadas, pues el control de la cadena queda relegada a un menor número de participantes. En ellas se hace especialmente importante definir con la máxima transparencia las reglas de uso entre los participantes. En estos casos, poder disponer del código permite comprobar que las correspondientes reglas, incentivos y medidas de protección están correctamente codificadas en la implementación de la blockchain.

Para que una blockchain consiga obtener el favor de sus participantes, éstos han de poder escrutar su funcionamiento interno. Esto a menudo se consigue mediante código abierto, pues si bien no es la única forma, el hecho de disponer del código de la cadena de bloques también favorece el desarrollo de nuevas innovaciones, su mantenimiento y la interoperabilidad con otras blockchains.

Sin embargo, hay que ser cauteloso con muchas de las iniciativas de las blockchains privadas que comercialmente se publicitan como «abiertas», pues en muchas ocasiones no son tan «abiertas» como pudiera parecer. Es habitual ver cómo muchas blockchains privadas liberan únicamente la parte de software cliente. En otras ocasiones, lo que se libera es simplemente una API que permite interaccionar con la cadena o incluso un Software Development Kit (SDK) para facilitar los desarrollos sobre su solución, pero sin delegar el control sobre el código clave del proyecto. Al igual que ocurre con el software libre y por ende con el código abierto, las soluciones basadas en modelos abiertos son mucho más difíciles de monetizar por compañías privadas, de ahí que muchas de ellas hayan trasladado su interés desde las blockchains puramente públicas hacia blockchains híbridas o privadas en las que poder rentabilizar nuevos modelos de negocio.

Más información sobre la relevancia del software libre y el movimiento de código abierto para las blockchains en <libroblockchain.com/codigo-abierto/>.

Capítulo 11

Seguridad y blockchain

Santiago Márquez Solís

Vivimos en un mundo inseguro, tanto que las cuestiones de seguridad representan una de las decisiones de inversión más importantes a las que debe enfrentarse cualquier empresa, grande o pequeña. Que esta cuestión no es una broma lo confirma el que en el año 2015 los gastos en seguridad superaran los 75.000 millones de dólares y, en 2016, los 81.600 millones. No obstante, y aun tratándose de una cifra enorme, muchas empresas, especialmente pymes, no invierten aún lo suficiente, lo que las convierte en el blanco preferido de los ataques. Sólo el gasto ocasionado por ataques de ransomware (programas que restringen el acceso a determinadas partes o archivos, y piden un rescate a cambio de quitar esa restricción) cuesta más de 325 millones de dólares al año. A más dispositivos conectados, mayor incertidumbre porque hay más potenciales focos de amenaza e incógnitas ante el comportamiento de esos mismos dispositivos.

Este último punto tiene una relevancia especial en el internet de las cosas (IoT), en el que se estima que tendremos más de 6 billones de dispositivos conectados en un plazo no superior a cinco años. No hay que olvidar que la interacción entre la tecnología blockchain y los dispositivos IoT es una de las grandes promesas de la primera, y que aún resuenan los estragos que, en octubre de 2016, provocó el ataque DDoS que dejó sin servicio a Dyn e hizo que muchas de las webs más importantes del planeta dejara de ser accesibles durante horas. De este suceso, que explicamos con más detalle en la sección de internet y blockchain de este libro, puede extraerse una valiosa lección respecto a la formación y divulgación de medidas de seguridad básicas entre los usuarios: el ataque a Dyn habría resultado más complicado de llevar a cabo si la herramienta utilizada, Mirai, no hubiera podido infectar a miles de máquinas configuradas, por defecto, con sus cuentas y contraseñas. Una lección que se puede sacar de esto es que cuantas más máquinas tengamos bajo nuestro control, mayor será el poder computacional para abordar ataques más sofisticados. El poder computacional es precisamente una de las bazas jugadas por algunas

blockchains, y en este sentido lo que asegura que la prueba de trabajo (Proof of Work, en inglés) tiene validez es que el poder computacional más grande está del lado de los nodos honestos que tratan de crear la cadena más larga y veraz para el sistema completo.

Una segunda lección señala que da igual lo fuerte que sea una cadena de bloques, si su eslabón más débil (el usuario final) está fuera de ella. Un usuario que concibe la seguridad como una mera cuestión de sensaciones, de *feeling*, escudándose en el recurrente «yo no tengo nada que ocultar», lo que hace es renunciar a su derecho a estar seguro. Tú puedes pensar que no eres importante, pero el análisis coordinado de miles de usuarios con determinadas pautas y conductas, y que renuncian voluntariamente a estar seguros, sí que lo es, y mucho.

Amenazas en el mundo de la blockchain

Cada vez aparecen nuevas técnicas que intentan que los sistemas revelen información. Estas amenazas están también presentes en las cadenas de bloques. He aquí algunas de ellas:

- **Ingeniería social:** si el usuario es el eslabón más débil, justo es considerar el medio habitual en el que se mueve como la principal amenaza. Facebook, Twitter, LinkedIn y el resto de plataformas permiten a los hackers acceder a gran cantidad de información e idear nuevas rutas de ataque. Si libero una dirección que uso habitualmente para pagos, es factible llegar a determinar mis movimientos de efectivo en una cadena de bloques como Bitcoin.
- **Servicios en la nube:** son un mecanismo muy útil para reducir costes y mejorar la escalabilidad de los sistemas de información, motivo por los que son cada vez más populares. Actualmente la tecnología de cadenas de bloques se vende como un servicio más en la nube. El llamado Blockchain as a Service (BaaS) es una tendencia en alza. La cadena de bloques no reside en ordenadores públicos o bajo el control de la infraestructura de la empresa, sino que está en ese lugar indeterminado que llamamos «nube». Por tanto, si se compromete la seguridad de la nube, se puede llegar a comprometer la seguridad de la cadena de bloques.

- **Bring Your Own Device** (BYOD)**:** «Traiga su propio dispositivo» (que eso significa BYOD en inglés) tiene mucho que ver con el IoT y la sensibilización de los usuarios acerca de la percepción que tienen de su seguridad. En muchos entornos es cada vez más común que los ordenadores no pertenezcan ni siquiera a la empresa y que estén conectados a otros recursos potencialmente valiosos para un atacante. Si pensamos en los elementos que incorpora un móvil (la cámara, la grabadora o el micrófono), un software malintencionado (malware) instalado en éstos podría dar acceso a información útil para atacar al sistema. Por eso, es imprescindible un usuario formado y concienciado en la importancia de tener sus sistemas de protección actualizados y activos.
- **Factores de riesgo internos:** se trata de ataques que no son realizados por hackers externos, sino por personas que trabajan dentro de las organizaciones y conocen las infraestructuras o aplicaciones que se usan. La existencia de puertas traseras (*backdoors*) que permitan, desde el exterior, acceder a los sistemas (código fuente público *versus* código fuente propietario) tampoco es de extrañar.

Reglas de seguridad y blockchain

Tradicionalmente, las medidas de seguridad persiguen preservar una serie de propiedades sobre el sistema en el que se aplican, propiedades que son válidas no sólo para las soluciones que se construyen sobre una cadena de bloques, sino también para la propia cadena de bloques. Las que explicamos a continuación son básicas:

- **Confidencialidad:** sólo los usuarios autorizados tienen acceso a la información y nadie más que ellos. En el ámbito de las cadenas de bloques privadas, solamente aquellos usuarios con los permisos adecuados y previamente autenticados deberían poder acceder a la información almacenada. Dado que las cadenas de bloques públicas permiten la consulta de la información registrada por cualquier tipo de nodo, el nivel de confidencialidad al que se ven sometidas es menor.

- **Integridad de la información:** es la garantía de que la información original almacenada no será alterada ni intencional ni accidentalmente. Esto significa que ninguno de los bloques, ni las transacciones que contienen, ni la historia de las mismas, puede ser alterada por ningún mecanismo. Aquí juega un papel decisivo el número de nodos que aseguran la información. Cuantos más nodos honestos existan, más difícil es para un atacante tener un poder computacional mayor que el resto de la red (ver más adelante el ataque del 51%) y, por tanto, más difícil es alterar la información y la historia de la cadena de bloques. Así se evita caer en un problema de integridad o de autenticación de actualidad (*no replay*), que consiste en probar que el mensaje es actual y que no se trata de un mensaje antiguo reenviado. Al llevar el histórico de todas las transacciones desde su puesta en marcha y disponer de un mayor números de nodos honestos, este problema quedaría resuelto. Esto se aplicaría tanto a cadenas de bloques privadas como públicas.
- **Autenticación de usuario:** es un proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser. La autenticación es complementaria a la confidencialidad y el paso previo que nos permite o no conectar con la cadena. Una vez que la conexión ha sido realizada, es posible el acceso a la información, pero no antes. La autenticación de usuarios en las cadenas públicas es un mero intercambio de parámetros de conexión, puesto que todos los ordenadores tienen el mismo derecho a usar la cadena y, por ende, a conectarse. En las cadenas privadas, la autenticación puede pasar por múltiples niveles de validación e intercambio de credenciales antes de poder realizarse el acceso. Esta situación es la que se produce cuando hacemos uso de plataformas (BaaS) y es la que tienen empresas como Microsoft Azure (con implementaciones privadas de Ethereum o Emercoin) o IBM BlueMix (con implementaciones privadas de Hyperledger Project, de la Fundación Linux).
- **Autenticación de remitente y del destinatario:** permite a un usuario certificar que el mensaje recibido fue enviado por el remitente y no por un suplantador. En las transacciones se conoce perfectamente quién las emite, quién las recibe y a quién pertenecen los diferentes tokens que circulan por el sistema. Hablamos de tokens porque es un modo más genérico del tipo

de información que se puede intercambiar en una cadena de bloques. En la red Bitcoin, el token clásico es la propia criptomoneda; en Ethereum, sin embargo, podríamos crear nuestros propios tokens, que bien pueden ser una moneda o la acción de una empresa. En este caso, la autenticación de remitente y destinatario debe quedar garantizada y saberse quién es el dueño de qué y cómo se transmite dicha propiedad.

- **No repudio en origen y en destino:** es decir, que cuando se reciba un mensaje, el remitente no pueda negar haberlo enviado ni el destinatario haberlo recibido. En las cadenas de bloques esta cuestión queda resuelta al disponer de todo el histórico de transacciones que se han producido desde su puesta en marcha. Cuando un nodo participa, debe aceptar las reglas que definen la lógica de funcionamiento de esa cadena y operar siguiendo esa lógica.

A todo este conjunto de reglas habría que añadir la accesibilidad, es decir, la capacidad de los sistemas de seguridad a ser lo más transparentes posibles al usuario y a no ser un estorbo que dificulte su operativa de trabajo. De lo que se trata, pues, es de llegar a un equilibrio entre la protección que esas reglas proporcionan y la facilidad de uso.

Los ataques clásicos a la blockchain

No podemos dejar de comentar los ataques clásicos identificados con esta tecnología y que ejemplifican, de un modo simple, la importancia de la seguridad en las soluciones basadas en cadenas de bloques. Cierto es que estos problemas se ponen de manifiesto con el desarrollo de Bitcoin, pero son ejemplos claros de cuestiones de seguridad que debe resolver una cadena de bloques pública:

- **El ataque del 51 % en las blockchains públicas:** ¿qué pasaría si los mineros se pusieran de acuerdo y se coordinaran para falsear la cadena de bloques? En primer lugar hablamos de coordinación porque para que lo que plantea esa pregunta sea factible es necesario tener justamente el 51 % del poder computacional de toda la red Bitcoin. Por qué un 51% y no un 50% es sencillo: si quiero llegar a falsear la cadena de bloques, necesitaré tener al menos la misma capacidad de cálculo que el resto de la red y

además un poquito más para poder ir generando los bloques falsos, darlos por buenos y anexarlos a la cadena de bloques. De esta manera sería mi cadena (y no otra) la que se consideraría buena. Con semejante poder se podrían revertir las transacciones o evitar las confirmaciones que se quisieran, hacer dobles gastos o cualquier otra travesura que se nos pase por la cabeza. Es decir, seríamos capaces de no hacer cumplir las reglas de las que hemos estado hablando anteriormente. Un ataque del tipo 51% no sólo afecta a Bitcoin, sino también a cualquier sistema descentralizado en el que se estén tomando decisiones por consenso.

- **La maleabilidad de las transacciones:** es un problema dentro de la implementación original de Bitcoin, actualmente superada por éste y otras soluciones, como Ethereum, pero que en su momento tuvo una gran repercusión. ¿En qué consiste? Hay información dentro de la transacción que está muy bien protegida, pero hay otros campos menos importantes que no lo están. Aprovechándose de esta debilidad, la maleabilidad de las transacciones consistiría en alterar el valor del hash de una transacción reciente autorizada, pero no confirmada, sin invalidar la firma. Esta transacción es a todos los efectos inválida. Ahora bien, si esta transacción llega a un nodo que hace minería y lo hace antes de que llegue la transacción válida, será la inválida la que quede registrada en los otros nodos.

Éstos no son los únicos modelos de ataques que existen, pero pueden servir como aviso de que la seguridad es importante y que no conviene nunca bajar la guardia.

Más información sobre cuestiones de seguridad y blockchain en <libroblockchain.com/seguridad/>.

Capítulo 12

Tecnologías blockchain

Luis Carlos García González, Manuel Polo Tolón e Íñigo Molero Manglano

La flexibilidad inherente a la blockchain posibilita un diseño exclusivo, acorde con las necesidades de los participantes. Así es como proliferan distintas propuestas con usos diferentes y de una forma transversal, tanto en el sector público como en el privado. La clave reside en entender la estructura de la cadena de bloques, y a eso es a lo que vamos a dedicar este capítulo, cuyo contenido incide en la operativa técnica de la blockchain de Bitcoin, considerada la referencia de base de todas las blockchains públicas.

La primera blockchain pública fue la de Bitcoin, todavía hoy un modelo de referencia para entender el funcionamiento de esta tecnología. Si se entiende éste será posible comprender también cómo funcionan otras muchas blockchains públicas y confrontar las conclusiones con las ventajas y debilidades que presentan las blockchains privadas o híbridas.

Todo empezó cuando, el 31 de octubre de 2008, un usuario entonces desconocido que se hace llamar Satoshi Nakamoto publicó un anuncio en la lista de correo de la página web <www.metzdowd. com>,[121] dedicada a criptografía. En él se contenía la descripción de un sistema de pagos que permitiría a sus usuarios proteger la propiedad mediante el uso de criptografía de clave asimétrica, así como evitar el doble gasto gracias a una base de datos descentralizada y validada por consenso a través de una prueba de trabajo que realizan los propios usuarios y tenedores de valor dentro del sistema. Lo novedoso de esta propuesta radica en que con ella ya no es necesaria la acción de un tercero de confianza que certifique y transfiera la propiedad digital. Aquí se halla el origen de lo que conocemos como blockchain. Todavía hoy, el control de la propiedad mediante el uso de la criptografía y el registro de la misma en una base de datos descentralizada aceptada por consenso conforman la espina dorsal de cualquier tecnología de cadena de bloques.

Una transacción con Bitcoin

Imaginemos a dos usuarios de Bitcoin, como pueden ser Satoshi Nakamoto y Hal Finney, éste un criptógrafo de PGP Corporation, que en 2004 creó un primer sistema de prueba de trabajo reutilizable (RPOW, en sus siglas en inglés). El 12 de enero de 2009 en el bloque 170, Hal se convierte en el primer receptor de una transacción de bitcoins. Satoshi pretende hacer entrega a Hal de unos bitcoins a modo de prueba para verificar que el software que ha hecho público unos días antes, el 9 de enero, interpreta correctamente su protocolo y ejecuta de forma eficaz las tareas para las que está diseñado: nodo de la red, minero encargado de realizar la prueba de trabajo o PoW (del inglés, *Proof of Work*) y monedero para gestionar y verificar el saldo del propietario. La red Bitcoin está dando sus primeros pasos. En aquellos momentos probablemente el cliente[122] de Satoshi y el de Hal eran los únicos nodos que conformaban la red Bitcoin. Sin embargo, para tener una mejor visión sobre cómo funcionan este tipo de redes descentralizadas de consenso vamos a suponer que aquel día de enero de 2009 una docena de cypherpunks usuarios de la lista de correo de metzdowd.com decide probar también el nuevo software.

En este escenario imaginario, la red está conformada por catorce nodos conectados gracias a internet y localizados en cualquier parte del mundo. Aunque Hal y Satoshi se conocen virtualmente, puesto que han mantenido correspondencia mediante correo electrónico, desconocen quiénes son las otras personas que han instalado el software diseñado por el segundo. Tan sólo pueden hacer una estimación del número de nodos de la red en función de los clientes que se conectan a ellos.

Cuando arranca la aplicación cliente de un usuario, ese nodocliente busca otros pares y el puerto por el que se comunican utilizando diversos mecanismos. Después, comprueba una base de datos con direcciones IP de pares a los que ha estado conectado en otras ocasiones. Si esta acción no funciona la primera vez que se ejecuta el nodo, también puede utilizar las IP proporcionadas por su usuario mediante un argumento en la línea de comandos de arranque de la aplicación o añadidas en su archivo de configuración. Otra alternativa sería emitiendo peticiones DNS[123] para descubrir las direcciones IP de otros pares. Si la petición DNS falla, el cliente usa las direcciones que tiene codificadas de

ciertos nodos semilla, aunque ésta es una alternativa de último recurso. Finalmente, independientemente de la posibilidad ejecutada, el cliente establece la primera conexión con otros pares mediante los mensajes «getaddr» y «addr». Así es como los clientes de Nakamoto y Finney acaban formando una red entre ellos, y lo mismo los del resto de criptógrafos que, según este ejemplo imaginario, están probando el software. En este caso, la altura del bloque actual es de 169, aunque la cadena de bloques consta de 170 bloques. La razón de tal diferencia es que el primer bloque de la cadena, conocido como «bloque génesis», comienza a numerarse por el número cero.

Pongamos ahora que Adam, uno de los criptógrafos que acaba de instalar el software de Satoshi, ejecuta por vez primera el cliente en su ordenador personal. Tras descubrir uno o varios pares y unirse a la red, lo primero que hace este nodo es reclamar a sus pares una copia íntegra de la cadena bloques, de modo que procede a su descarga y verificación. Éste es un paso crucial en un sistema descentralizado como Bitcoin ya que cada nodo valida de forma independiente y sin necesidad de confiar en ningún otro la integridad de todas las transacciones. Este proceso inicial es lento y se hace más lento aún a medida que crece el tamaño de la cadena, pero es básico si una cadena quiere gozar de buena salud. Sin embargo, aunque el mecanismo verifica la propiedad de las criptomonedas deja aún pendiente un problema importante: cómo descartar un posible intento de «doble gasto».

Cuando Satoshi se sienta frente a su ordenador para confirmar el pago que va emitir, la red sobre la que se asienta su sistema es minúscula, pero plenamente funcional. En nuestro ejemplo sólo existen catorce partícipes-nodos, pero nos sirve como una muestra totalmente representativa para ilustrar el funcionamiento de la red. Los fundamentos están presentes y permanecen inalterables, independientemente del número de participantes.

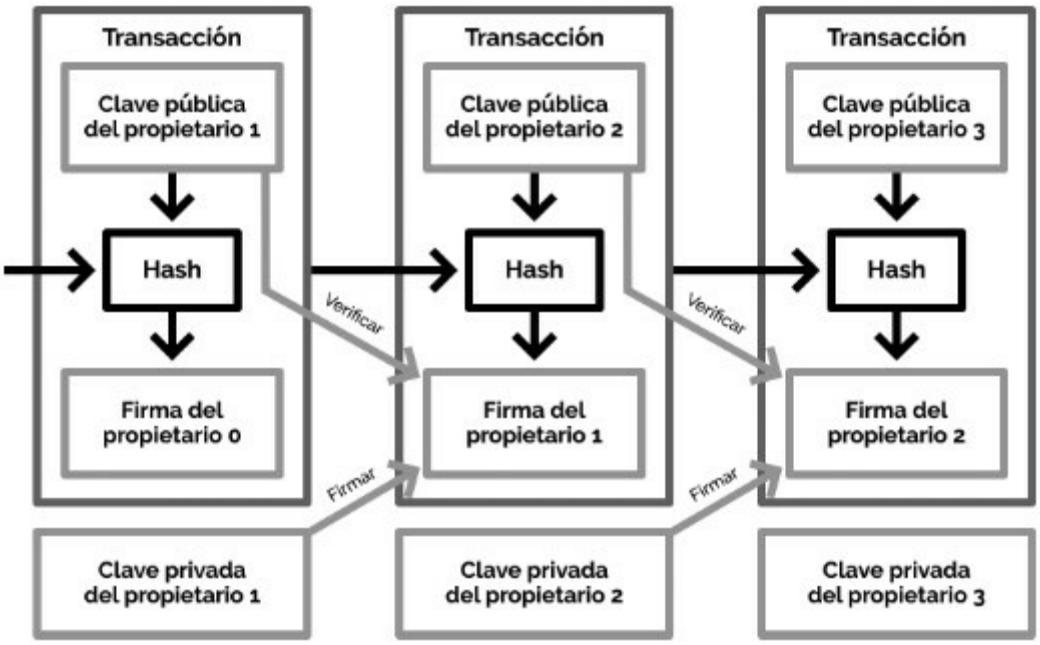
Satoshi tiene el nodo sincronizado con sus pares en el bloque 169 y dispone de muchas criptomonedas bitcoin para gastar, puesto que su ordenador ha estado generando bloques para conformar la cadena, exactamente desde el 3 de enero de 2009, fecha en la que arranca el software que ha desarrollado él mismo y produce el bloque génesis. Pero antes de seguir adelante, una curiosidad: en ese bloque cero incluye el texto *«The Times 03/Jan/2009 Chancellor on brink of second bailout for banks»*,[124] toda una declaración de

intenciones. Por aquel entonces, cada bloque que alguien añade a la cadena es recompensado con 50 nuevos bitcoins que se emiten en ese instante. Esta operación se repite cada 10 minutos porque así se ha diseñado el software. Ya que inicialmente el único nodo que conforma la red es el que ejecuta Nakamoto, todos los bitcoins de nueva creación acaban en el monedero que gestiona su cliente. Pero estos primeros bitcoins no se pueden gastar inmediatamente, porque se requiere de un período de maduración de 100 bloques. Es necesario que la cadena crezca hasta esa altura antes de poder transferirlos. Con esta precaución se pretenden evitar situaciones de pagos no aceptados en el caso de ramificaciones o bifurcaciones (*Forks*) temporales de la cadena.

La firma de una transacción de Bitcoin

¡Todo está listo! Es el momento de probar que el sistema es eficaz. No obstante, es tan sólo una prueba de concepto, pues los 10 bitcoins que va a transferir Nakamoto no tienen absolutamente ningún valor de mercado. ¿Quién estaría dispuesto a ceder algún tipo de bien a cambio de una simple anotación que se replica en una serie de máquinas a cargo de un software que no controla nadie? Pero es un instante mágico que supone una ruptura con la historia económica que conocemos. Satoshi toma unos bitcoins minados[125] en el bloque 9 porque ya tienen suficiente tiempo de maduración. La dirección a la que están asignadas es la 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S. Esta dirección contiene la única transacción de ese bloque, la «transacción coinbase» (o recompensa), que son 50 bitcoins de nuevo cuño. Todos los nodos sincronizados han comprobado la validez del bloque y de los datos contenidos en él. El dinero electrónico puede definirse así como una cadena de firmas digitales en la que los propietarios transfieren la propiedad firmando digitalmente un hash de la transacción previa junto con la dirección del nuevo propietario. La clave privada permite realizar la firma de la transacción y supone el control del saldo contenido en su dirección correspondiente. Entretanto, la clave pública del propietario que transfiere los fondos se da a conocer en el mismo proceso, de forma que el resto de los agentes verifiquen con ella la firma digital y den por bueno que el que ordena la transferencia de propiedad es el dueño legítimo de los bitcoins.

Cadena de firmas digitales en transacciones de Bitcoin.



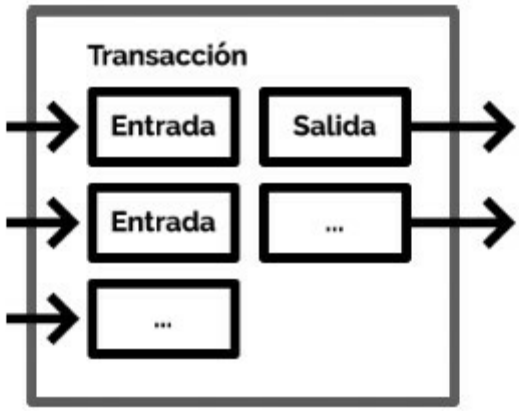
Las transacciones en Bitcoin consisten simplemente en una serie de entradas (*inputs*) —que son salidas (*outputs*) de transacciones anteriores—, que fusionan todos sus saldos en bitcoins en una o varias nuevas salidas. Son agrupadas dentro de los bloques y, puesto que no van cifradas, son fácilmente legibles para todos aquellos que tengan acceso a la cadena.

El saldo contenido en los *inputs* seleccionados se utiliza completamente, de forma que si la suma total de saldos incluidos en los *outputs* es inferior a la de los *inputs*, la diferencia se considera como comisión (*fee*) y se utilizará para incentivar el mantenimiento de la red. También es interesante detallar que tanto las entradas como las salidas contienen un campo llamado *ScriptPubKey* que permite utilizar en Bitcoin un sistema personalizado de guion de comandos (*scripting system*) que posibilita diseñar distintos tipos de transacciones complejas que se pueden vincular mediante acuerdos criptográficos. Son la primera implementación de los «contratos inteligentes» explicados en la sección de aplicaciones transversales.

Esto es lo que realiza Satoshi en este momento: toma como entrada la salida de 50 bitcoins hacia la dirección 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S del bloque 9, añade como primera salida la dirección Bitcoin 1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3 de su destinatario Hal, especificando que le serán transferidos 10 bitcoins. Utiliza una segunda salida para los 40 bitcoins restantes que son enviadas como «cambio» a otra dirección

Bitcoin bajo el control de Nakamoto. Firma estos datos con la clave privada correspondiente a su dirección 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S e incluye al conjunto de datos resultante la clave pública de dicha dirección para que cualquier nodo que reciba la transacción pueda certificar que, como legítimo propietario, está capacitado para ordenar el trasvase de fondos. A continuación, retransmite el conjunto de datos a los pares conectados directamente a su nodo. Éstos a su vez repiten el proceso enviando la transacción a los pares que desconozcan el anuncio, y así hasta que se recubra la red por completo.

Modelo de transacciones con entradas (inputs) y salidas (outputs).



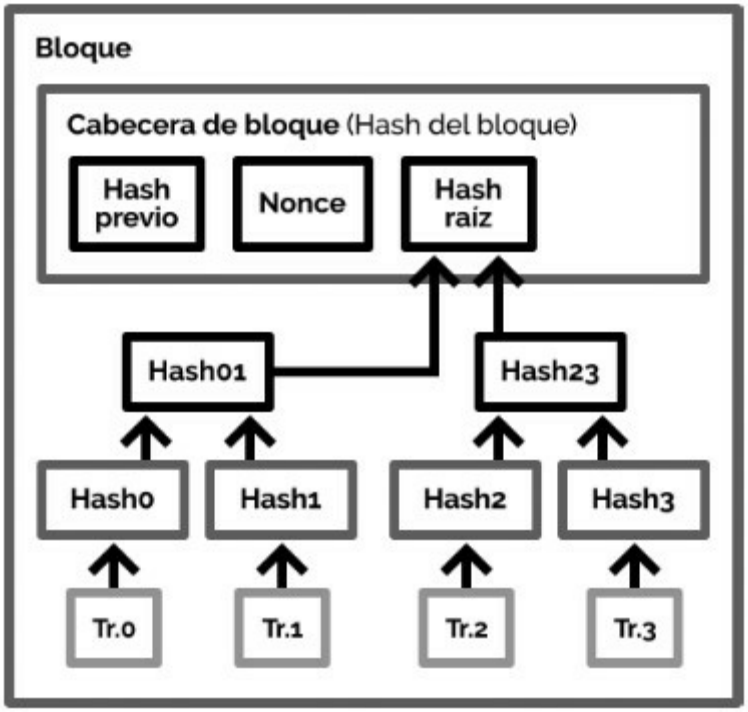
La transacción bitcoin no es firme, hay que esperar la confirmación

Mientras los nodos reciben la transacción de Satoshi a Hal, todos intentan descubrir un nuevo bloque válido para la cadena. De hecho están constantemente trabajando en la búsqueda del siguiente bloque, es una pelea/competencia constante cada 10 minutos. El programa cliente de Hal recibe de sus pares la transacción emitida por Satoshi, agregando 10 bitcoins más al saldo global de su monedero, pero avisando de que carece de confirmaciones.[126] Hal advierte así que Satoshi ha solicitado a la red la transmisión de cierta cantidad de bitcoins a una dirección de su propiedad porque ya tiene en su poder la firma digital realizada con la clave privada de Satoshi. Es decir, que éste autoriza la transferencia de 10 bitcoins a la dirección que Hal le proporcionó mediante un correo. Pero mientras no tenga confirmaciones, mientras la transacción no sea incluida en un bloque que forme

parte de la cadena, Hal no puede considerar que ya ha recibido los bitcoins. De hecho, durante este tiempo los bitcoins siguen perteneciendo a Satoshi porque en la red aún no se han movido de su cartera. Todo esto significa que lo que se ha producido hasta ahora no es más que una especie de anuncio o solicitud pública de transacción a la red que se está procesando.

El diseño de Satoshi estableció que la red debería realizar un determinado esfuerzo computacional durante 10 minutos de media, antes de que se diese el hallazgo de un nuevo bloque. Como estos eventos siguen una distribución de probabilidad de Poisson tenemos que el tiempo medio de aparición de un nuevo bloque, independientemente del momento en que hagamos la observación, será siempre de 10 minutos de media. Ése será el tiempo medio requerido para que se confirme cualquier transacción que sea incluida en el siguiente bloque descubierto. Y en este caso, eso es lo que está esperando Finney.

Hasheado en un árbol de Merkle en Bitcoin.



La unidad que conforma la cadena se conoce como «bloque». Éste se estructura en dos partes: la cabecera del bloque y el Merkle Tree o árbol de Merkle de las transacciones o datos de valor, según el tipo de blockchain sobre la que tratemos. La cabecera del bloque a su vez está compuesta por el hash del

bloque antecesor, un contador llamado «nonce» y el hash raíz del árbol Merkle de todas las transacciones incluidas. Yendo más al detalle, observamos el bloque estructurado en cinco campos:

1. **Número mágico** (4 bytes): para Bitcoin siempre toma el valor 0xD9B4BEF9. Es un identificador de la estructura del tipo de datos o archivos que le siguen. Es elegido arbitrariamente por el creador del protocolo.
2. **Tamaño del bloque** (4 bytes): determina el número de bytes máximo contenidos en el bloque, exceptuando estos dos primeros puntos.
3. **Cabecera del bloque** (80 bytes): constituido por seis elementos:
    a. *Versión* (4 bytes): detalla la versión del bloque.
    b. *Hash del bloque antecesor* (32 bytes): hash de 256-bits de la cabecera del bloque anterior.
    c. *Raíz del árbol de Merkle* (32 bytes): contiene el hash de 256bits del nodo raíz del árbol Merkle de transacciones.
    d. *Tiempo* (4 bytes): marca temporal con el momento de creación del bloque en segundos.
    e. *nBits* (4 bytes): valor de la dificultad requerida para generar el bloque.
    f. *Nonce* (4 bytes): es un contador que permite, variando su valor, obtener hashes de la cabecera del bloque para encontrar el próximo bloque válido.
4. **Cantidad de transacciones** (1-9 bytes): es un valor entero positivo y detalla el número de transacciones contenidas en el bloque, incluida la transacción coinbase.[127]
5. **Transacciones** (número de bytes limitado por el tamaño máximo de bloque): listado de todas las transacciones incluidas en el bloque, que deben aparecer en el mismo orden utilizado para generar su árbol de Merkle correspondiente. Este campo no puede estar vacío, al menos ha de contener la transacción coinbase.

Como cada cabecera de bloque incluye el hash de la cabecera del bloque previo y a su vez es utilizada para conformar la cabecera del bloque sucesor, obtenemos una estructura que podemos asimilar a una cadena. De ahí el origen del nombre. La concatenación de firmas (hashes) supone que cualquier alteración que se produzca en los datos contenidos en el cuerpo del bloque o en su cabecera generará una alteración del hash final de ésta, bien por transferencia en cascada de la modificación de los hashes a través del árbol de Merkle, bien por cambios en la propia cabecera de bloque. Esta modificación se transmite igualmente a todos los bloques sucesores del alterado, recorriendo desde éste el resto de la cadena hasta el bloque más moderno, una acción esta fácilmente detectable por cualquiera de los nodos que reciban la cadena perturbada. Los nodos honestos rechazarán cualquier intento de manipulación de los datos, lo que evita la replicación del bloque mutado a través de la red de pares. De este modo tenemos a todos los nodos conectados a nuestra minúscula red Bitcoin haciendo pruebas de ensayo y error para dar con un hash que valide la Prueba de Trabajo o *Proof of Work* requerida. Pero ¿en qué consiste la Prueba de Trabajo y cuál es su objetivo?

Una Prueba de Trabajo para eludir el problema del doble gasto

La Prueba de Trabajo (PoW, por sus siglas en inglés) consiste en realizar un esfuerzo computacional determinado en el protocolo, con el objetivo de impedir que los nodos maliciosos incluyan bloques fraudulentos en la cadena. Mientras que el trabajo para obtener un bloque válido —y cobrar la recompensa— puede suponer un elevado coste de tiempo para la unidad central de procesamiento de un equipo informático (CPU) y no menos de energía consumida, la verificación de que el bloque es correcto es inmediata para cualquier ordenador doméstico.

En Bitcoin se hace uso de la función *hashcash*, ya explicada en el capítulo de criptografía. Se trata de un algoritmo que requiere de tres parámetros para funcionar y adaptarse a Bitcoin:

1. **Cabecera de bloque:** está conformada por los seis campos expresados en el apartado anterior.

2. **Nonce:** un número de 32 bits que se va modificando secuencialmente para obtener salidas de la función hash distintas. Puesto que este número es pequeño, cuando se agota se hace necesario modificar algún dato de los puntos 1 o 3.

3. **ExtraNonce:** forma parte de la transacción especial llamada coinbase y se modifica cuando se han usado todos los posibles valores del nonce. Su variación requiere recalcular todos los nodos de la rama izquierda del árbol de Merkle, pues la transacción coinbase se sitúa siempre en el nodo más a la izquierda del árbol.

El esfuerzo requerido para encontrar una solución válida a la Prueba de Trabajo podemos considerarlo independiente del número de transacciones que se incluyan en el bloque, ya que, una vez calculado el valor del nodo raíz del árbol de Merkle, todos los mineros (es decir, aquellos participantes de la red que mantienen un nodo ejecutando la prueba de trabajo que requiere la red) aplican la misma función hash sobre un conjunto de datos estandarizado de 80 bits. El cálculo requerido por dicha función sobre un grupo de bits de la misma extensión es el mismo para todos. Lo único que cambia es el esfuerzo computacional cuando se agota el parámetro nonce, de forma que, para no volver a obtener hashes repetidos, es necesario modificar el valor extranonce que varía la rama izquierda del árbol de Merkle. Una vez obtenido el nuevo valor del árbol se vuelve a recorrer secuencialmente el número nonce para tratar de obtener un bloque válido.

Pero ¿qué se entiende por encontrar un bloque válido? Encontrar un bloque válido significa dar con un resultado de la función hashcash —recordemos que consiste en un número de 256 bits que podemos ver en los exploradores de bloques[128] expresado en formato hexadecimal— a partir de los datos de entrada particulares de nuestro bloque, cuyo valor sea inferior al exigido por la red para dicho momento y que está expresado en el campo Target de la cabecera. Las funciones hash parecen mostrar un carácter aleatorio o no determinista, de tal forma que necesitaremos aplicar la función un número indeterminado de veces hasta obtener un valor menor al solicitado. El mecanismo es similar a arrojar un dado con, supongamos, un millón de caras y que nos requieran una tirada menor o igual a mil. De media, necesitaremos

lanzar el dado mil veces hasta dar con un valor que verifique el criterio requerido. Además, podemos modificar el valor mínimo para facilitar la tirada, o no. Esto es lo que hace la red bitcoin constantemente, también ahora mismo.

Mientras los mineros ensayan muchos pases de la función hash hasta dar con uno bueno, su verificación sólo necesita uno. Este punto es de vital importancia, ya que el libro contable que es la blockchain de Bitcoin no puede ser escrito por cualquiera: cada nueva página —es decir, cada nuevo bloque— contiene un sello, una huella de la página anterior, la página que agrega y la firma del minero con la prueba de trabajo. De este modo, si algún malintencionado intenta hacerlo fraudulentamente, su bloque corrupto no superará la verificación del hash y será rechazado por el resto de nodos. Como los propietarios de nodos que minan están dedicando recursos en forma de energía y tiempo de cómputo a favor de la red, ésta incentiva su trabajo con la creación de bitcoins con los que son recompensados. Puesto que en estos inicios es muy fácil dar con un bloque, el ordenador de Adam, que hace poco ha pasado a formar parte de la incipiente red Bitcoin, da con un hash inferior al exigido por la red y envía su nuevo bloque —el número 170 ya— a los pocos pares a los que está conectado. Éstos verifican que el hash es menor al que establece la red y, a su vez, lo retransmiten a los pares que no lo hayan recibido hasta que el último bloque alcanza a toda la red distribuida. En este bloque, Adam, ha incluido la transacción que emitió Satoshi a Hal y, como ha pasado a formar parte de la cadena, Hal puede ver que se ha confirmado; es decir, que ha sido incluida en un bloque. Con cada bloque que crezca la cadena su transacción pasará a sumar una nueva confirmación. Y así indefinidamente.

Incentivos para la minería en Bitcoin

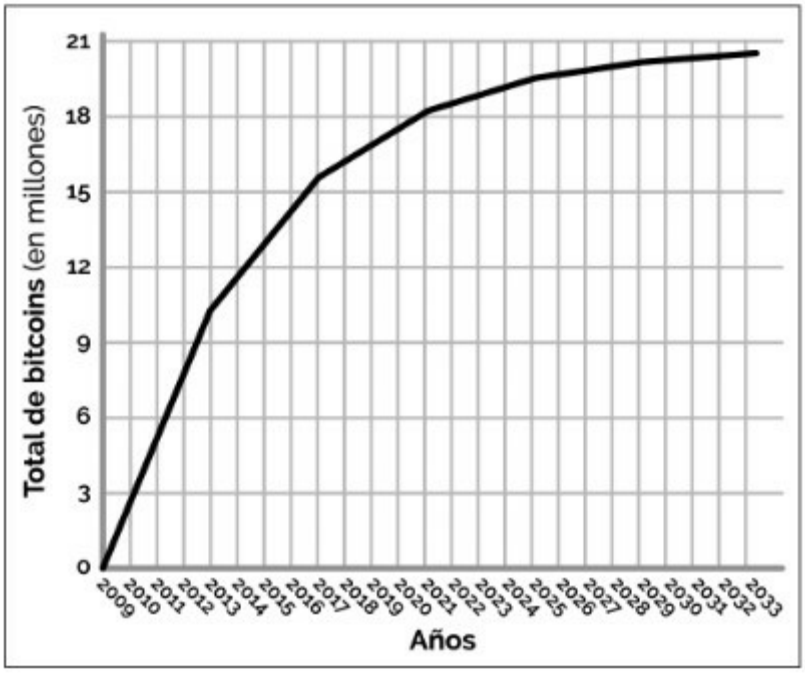
Adam también está feliz porque ahora dispone de 50 BTC o bitcoins con los que hacer pruebas. El bloque 170 sólo contiene dos transacciones, la de Satoshi que va en segundo lugar y la transacción especial conocida como coinbase. Gracias a ella, el protocolo ha asignado, sin la necesidad de ninguna transacción previa, de ningún input, que dispusiera de ese saldo de 50 BTC en una dirección propiedad de Adam.

Como ya sabemos, el protocolo marca que los bloques se deben resolver a un ritmo medio de 10 minutos. Este valor ha sido elegido por Satoshi al programar la primera versión del cliente y se mantiene hasta nuestros días. Uno de sus propósitos es el de emitir masa monetaria de forma predecible en el tiempo. Además, el protocolo también establece que cada 210.000 bloques el premio se reduzca a la mitad manteniendo la oferta limitada en el tiempo —a semejanza del oro— a 21 millones de unidades.

$$
\begin{aligned}
N &= 210.000 \times \left(50 + \frac{50}{2} + \frac{50}{4} + \frac{50}{8} + \ldots\right) \\
&= 210.000 \times 50 \times \left(1 + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots\right) \\
&= 210.000 \times 50 \times 2 \\
&= 21.000.000
\end{aligned}
$$

La suma contenida dentro de los paréntesis representa las reducciones del premio cada cuatro años de media para un tiempo ilimitado. Es una serie matemática convergente, lo que significa que, a pesar de tener infinitos sumandos, su suma total es finita y que para este caso particular vale 2. De esta forma tenemos una emisión máxima limitada al doble de los bitcoins entregados durante los primeros cuatro años: 210.000 bloques a 50 BTC cada uno.

Distribución de bitcoins en el tiempo.



Como el código de programación es de libre acceso —software libre—, estas reglas son auditables por cualquiera y su alteración visible a todos, de modo que sólo se podrían modificar bajo consenso mayoritario de los partícipes de la red. Es por lo que se puede afirmar que nadie tiene la potestad de modificar por su cuenta el límite de emisión de esta moneda digital y que no será admitida cualquier variación de las reglas establecidas en el protocolo que perjudique a la mayoría.

En este instante primigenio, la entrega de bitcoins no parece más que un interesante mecanismo de repartición inicial de unidades. Pero, en realidad, el concepto va mucho más allá. A partir del punto en el que pasan a cobrar valor monetario, la red utiliza la emisión de bitcoins como un sistema de defensa ante posibles atacantes. El sistema, además, sólo utiliza los recursos que necesita y no más. Si el precio de los bitcoins es barato, la red no será un objetivo de ataque por ser poco interesante, y como apenas existen incentivos habrá pocos usuarios motivados como para ceder recursos de sus máquinas en favor de la red. Sin embargo, si el valor de los bitcoins crece mucho, también aumentará el posible lucro de un ataque exitoso. Entretanto, la posibilidad de rendimientos económicos altos por la obtención de nuevos bitcoins valiosos, llevará a muchos mineros a aumentar la potencia entregada para lograr un trozo mayor en el reparto de las recompensas, transformando la red, a su vez, en un sistema mucho más difícil de atacar.

Cuando la potencia de cálculo de la red aumenta —equivale a tirar el dado un mayor número de veces por segundo—, disminuye el tiempo que se tarda en dar con un hash menor al exigido, lo que provoca que los bloques se generen con un período inferior a los 10 minutos diseñados. La consecuencia de esto es que la emisión monetaria se acelera. Como sucede lo contrario si la potencia disminuye, para cumplir con el objeto de mantener predecible en el tiempo la emisión de moneda, cada 2016 bloques (unas dos semanas a 10 minutos por bloque), la red recalcula la dificultad de dar con un hash válido según el tiempo que se han tardado en generar los 2016 bloques anteriores, de tal forma que el tiempo medio por bloque se ajuste de nuevo a los 10 minutos.

A medio y largo plazo, la creación de bitcoins como incentivo para los mineros irá perdiendo importancia. El sistema, sin embargo, tiene ideado otro mecanismo para conseguir que los mineros continúen aportando recursos. El

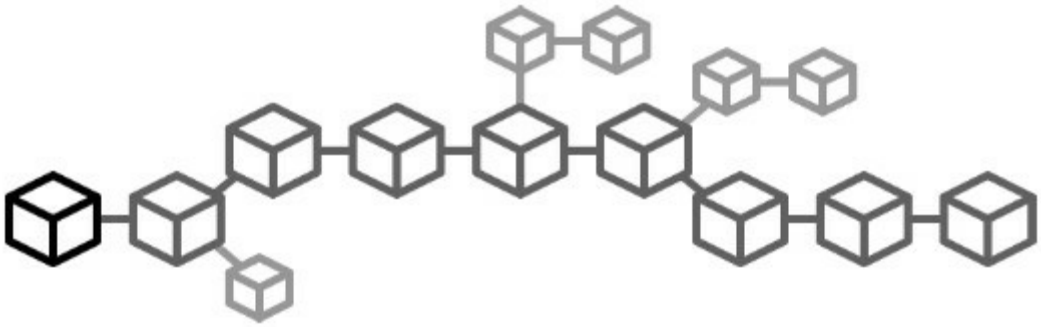
saldo de la transacción coinbase está compuesto por los nuevos bitcoins creados más la suma de todas las comisiones que paguen las transacciones que se incluyan en el bloque. Puesto que los mineros no tienen la obligación de incluir transacciones en los bloques —excepto la transacción coinbase—, pueden escoger sólo aquellas que paguen la comisión más alta por ejecutar el registro. Esto proporciona una forma de dar prioridad a una transacción frente a otras con poca o nula comisión. En situaciones de alta demanda de la red, el tiempo de ejecución requerido para la confirmación de una transacción es fuertemente dependiente de la comisión que se pague. En un escenario exitoso para Bitcoin, con un uso generalizado de la red, las comisiones por transacción deberían acabar siendo la fuente de ingresos principal de los mineros.

Dos bloques simultáneos en la red Bitcoin

En nuestro escenario supuesto, Adam ha encontrado el bloque 170, pero muy poco después el nodo de Wei —otro de los criptógrafos que conforma la red— da con un hash inferior al requerido para su propia versión del mismo bloque, que automáticamente distribuye entre sus pares.

Recordemos que nuestra cadena de bloques es una base de datos distribuida que contiene el registro contable del sistema y está formada por una serie de grupos de datos enlazados a los que llamamos precisamente «bloques». Este conjunto es ordenado. Cada bloque siempre cuenta con único bloque antecesor. No ocurre lo mismo con los bloques sucesores (y esto es un detalle de principal trascendencia para este tipo de tecnología), ya que cualquiera de ellos, durante cierto tiempo, puede tener uno o varios aspirantes. En el caso de un único sucesor, que suele ser lo habitual y lo deseable, la estructura de cadena es evidente; sin embargo, en ocasiones más o menos frecuentes según los parámetros elegidos en el diseño inicial, pueden aparecer dos o más bloques hijos siendo ambos válidos hasta que se alcance un consenso que determine cuál de ellos será el aceptado.

Modelo de una cadena de bloques o blockchain en Bitcoin.



Para este caso de aparición de dos bloques sucesores a uno previo, Satoshi propone que los nodos trabajen para hallar el siguiente bloque válido sobre el primero que reciban, pero que almacenen temporalmente también el segundo o sucesivos hasta que se resuelva el dilema. Así, del total de los doce nodos de nuestra red es posible imaginar a nueve trabajando sobre la versión del bloque 170 de Adam, que ha alcanzado más nodos porque se ha generado antes, y otros tres haciendo lo mismo sobre el candidato de Wei. El dilema se deshace cuando alguno de los grupos genera un nuevo bloque candidato válido que retransmite al resto de los nodos.

Hasta su resolución, la cadena de bloques está ramificada, puesto que parte de la red trabaja en hallar el bloque sucesor de un candidato, mientras que la otra facción trabaja sobre un candidato distinto. La velocidad de transmisión de los datos a través de los nodos cobra aquí relevancia junto con el volumen de datos transmitidos o tamaño del bloque, ya que bloques más grandes implican transmisiones más lentas de los mismos. En este escenario, el bloque candidato con mayor difusión temprana tiene más posibilidades de formar parte de la cadena definitiva, puesto que tendrá una mayor base de partícipes trabajando sobre él para lograr el próximo bloque candidato. Esto desincentiva la creación de bloques grandes si el tiempo medio de transmisión al resto de los nodos de red no es despreciable frente al tiempo esperado de aparición de nuevos bloques —elegido por diseño de la cadena—, lo que plantea problemas de escalabilidad. Es decir, para redes lentas no podemos tener bloques grandes con tiempos cortos de hallazgo de nuevos bloques sin que la cadena esté continuamente bifurcándose y generando cadenas secundarias que dejarán de ser válidas, por consenso, en cuanto una de ellas alcance una longitud superior al resto. Una situación esta que finalmente conduce a tener que esperar a que la cabeza de la cadena se aleje lo suficiente de un bloque determinado como para poder

considerar su información no alterable. Estos bloques que conforman las ramificaciones abandonadas de la cadena se conocen como «bloques huérfanos».

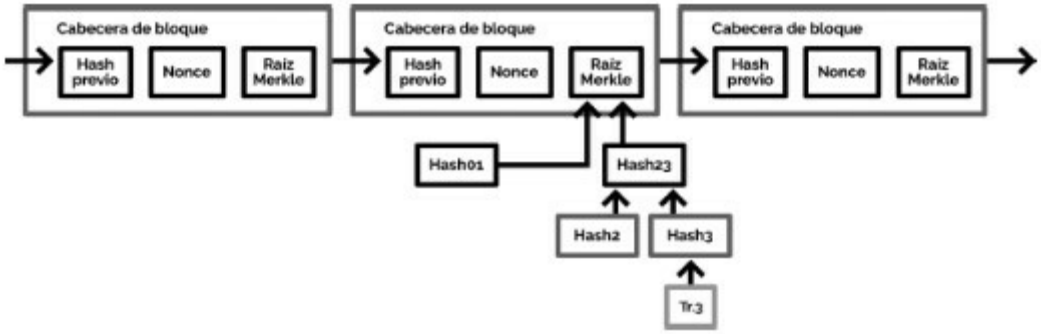
Las bifurcaciones compuestas por un número importante de bloques son indeseables y conducen a inestabilidades del sistema. Éstas se pueden producir de forma indeseada por errores de programación en los nodos o de forma intencionada, en el caso de que se altere por decisión de los desarrolladores principales del código alguna característica del protocolo y permanezcan nodos sin actualizar a la nueva versión. Existen dos tipos de bifurcaciones, conocidas por su terminología en inglés como *softfork* y *hardfork*. La primera de ellas es una modificación que no requiere de actualización de los nodos con versiones antiguas y es más sencilla de hacer porque sólo es necesaria una mayoría de mineros que acepten las nuevas reglas. En el caso del *hardfork*, todos los nodos antiguos se vuelven incompatibles con las nuevas reglas del protocolo y rechazarán los bloques que se produzcan bajo la nueva versión. Así, un *hardfork* implica la actualización obligatoria de todos los nodos, lo que requiere un consenso casi total de los partícipes de la red. En caso contrario, la cadena progresará con dos ramas separadas e incompatibles entre sí, una situación que se debe evitar a toda costa.

Entretanto, Nick, uno de los pares de Adam, que lleva trabajando sobre el bloque de éste casi desde su aparición, pues lo recibió directamente de su ordenador, da con un hash válido para el bloque 171 que su nodo comienza a distribuir. Al poco, el nodo de Adam, que está emparejado directamente al de Nick, recibe el nuevo bloque, pasa a distribuirlo y comienza a calcular hashes sobre la cabecera de éste para dar con un resultado válido que suponga el 172. Paralelamente, Wei continúa trabajando sobre su versión de bloque 170, pero uno de sus pares le envía el reciente bloque 171 descubierto por Nick que «cuelga» del bloque 170 de Adam. Ahora, la versión más larga de la cadena tiene una altura de 171, el nodo de Wei verifica la validez del bloque, desestima su bloque 170 y pasa a buscar el 172 a partir del bloque de Nick. Lamentablemente ha de renunciar a los 50 bitcoins que le hubiese proporcionado su versión de bloque 170, pero no le queda otra opción, porque el resto de la red lo rechazará.

Sucesos encadenados en el tiempo en la red Bitcoin

Lo que pretende lograr todo este proceso es una estructura de datos ordenados en el tiempo. La información contenida en cada bloque es «sellada» con una marca temporal que permite determinar que es previa a la incluida en cualquiera de los bloques que cuelguen de éste. Es lo que se entiende como «servidor de sellado de tiempo». Para Bitcoin, el objetivo es tener una línea temporal continua de propiedad de las criptomonedas, desde la generación de éstas hasta la dirección destinataria actual. El análisis mediante funciones hash y estructuras de árboles de Merkle permite a los nodos y, por tanto, al destinatario final de las mismas, verificar que no está siendo objeto de un envío fraudulento o doble gasto.

Verificación de pagos simplificada en la cadena de prueba de trabajo más larga.



Debido al sistema propuesto, un nodo o grupo de nodos maliciosos no puede generar nuevas monedas ni usar aquellas de las que no controle sus claves privadas. Sin embargo, sí podría intentar enviar los mismos bitcoins a dos destinatarios distintos. Para ello sería necesario que intentase pagar con los mismos inputs a outputs distintos en dos ramas diferentes de la cadena. El grupo de nodos deberían construir una rama más larga que el grupo de nodos honestos, de forma que éstos acepten su versión por ser mayor. La primera transacción quedaría así en una rama huérfana y el intento de doble gasto fructificaría.

Las posibilidades que tiene el atacante de producir una rama más larga que el resto de la red mediante la concatenación de hallazgos aleatorios de nuevos bloques decae de forma exponencial a medida que se aleja la cabeza de la cadena del punto de intento de fraude. La forma que tienen los destinatarios de

las transacciones para que las probabilidades de éxito de un ataque de este tipo sean minúsculas consiste en no dar por bueno el pago recibido hasta que se supere un determinado número de confirmaciones de la transacción por parte de la red. La opinión generalizada dice, que una vez se alcanzan las seis confirmaciones, el riesgo de doble gasto es despreciable, lo que para Bitcoin supone esperar aproximadamente una hora desde la confirmación de la transacción.

Todo esto cambia si el atacante de la red controla más de un 51 % de la potencia computacional. En nuestra pequeña red inicial de catorce nodos, considerando equipos con prestaciones similares, una alianza de siete de ellos permitiría que este grupo fuese capaz de generar ramas mayores de la cadena, realizar anuncios de transacciones en los bloques que encuentra el grupo menor de nodos honestos y generar una versión más larga con las transacciones modificadas. A esto se lo conoce como el «ataque del 51%» y es una de las formas teóricas de destruir la confianza en la red. Por ello es relevante la acumulación de esfuerzo computacional dedicado a la blockchain de Bitcoin y su mayor dispersión posible.

Transacciones públicas en Bitcoin

El modo que tienen nuestros criptógrafos de mantener a salvo la privacidad de las transacciones y el saldo de las carteras se apoya en el hecho de que no es necesario tener ningún contacto con la red para generar una nueva clave privada con su dirección asociada. Puesto que la clave privada no deja de ser más que un número aleatorio de 256 bits, cualquiera puede producirlas de forma ilimitada y sin tener que ceder ningún dato personal para ello. Los saldos de las direcciones son visibles para todos los usuarios con acceso a la cadena de bloques, pero no pueden asociarlas a ninguna persona en concreto. Para ello es necesario que el propietario de una dirección haga pública de alguna forma su relación con la misma. Una vez establecida esta relación existe cierta posibilidad de trazar el recorrido de los saldos de una determinada dirección para conocer futuros o anteriores propietarios. La recomendación es usar constantemente direcciones creadas ex profeso para recibir nuevas transacciones y no reutilizar direcciones a fin de mantener la privacidad del usuario lo más a salvo posible.

Esto ha hecho que se hable de Bitcoin como una «red seudónima» en la que los usuarios están tras las direcciones, y no «anónima», en la que no serían visibles ni los saldos ni las direcciones.

Las blockchains públicas y sus principales diferencias

Todas las blockchains públicas han de estar construidas sobre software libre, pues sólo así tenemos la garantía de que nadie podrá ser excluido de ellas. Lo más importante, sin embargo, es que al estar el código de programación disponible para todo el mundo, los mecanismos que podrían establecer restricciones de cualquier tipo resultan ineficaces.

Con el éxito de Bitcoin muchos desarrolladores se han lanzado a modificar su protocolo, aprovechando que es público, su código está disponible y permite la modificación. Estos desarrolladores han buscado alterar determinadas propiedades sometidas a discusión o, a su entender, débiles con el fin de obtener alternativas a Bitcoin que ofrezcan otras características demandadas entre ciertos sectores de usuarios. También se da frecuentemente el caso de apariciones de meros clones de Bitcoin, sin ningún aporte real al desarrollo de esta tecnología, generalmente orientados a entornos geográficos particulares o sectores específicos de actividad económica. En estas circunstancias, lo más probable es que el objetivo real de sus creadores sea, simplemente, atraer a un determinado grupo de usuarios dispuestos a invertir en su criptomoneda, lograr un éxito relativo con el que rentabilizar su posición inicial de privilegio como partícipes de las fases iniciales de la tecnología o *early adopters*, y enriquecerse de forma rápida y sencilla. Este tipo de modificaciones del protocolo deriva en cadenas incompatibles que surgen al calor del éxito de Bitcoin y llevan una existencia paralela a éste. Se hace público su software, se lanza el bloque génesis de su versión de blockchain y aquellos interesados pasan a formar parte de su red y a negociar sus tokens en el incipiente mercado que se establezca.

El nexo común de todas estas tecnologías es la estructura de cadena. Pues bien, sin alterar ésta, el protocolo de Bitcoin admite diversas modificaciones tanto de configuración como de diseño. Las podemos agrupar según el tipo:

1. **Tiempo por bloque:** por lo general se trata de reducir el tiempo que se requiere para cada confirmación de la red a fin de disponer de transacciones instantáneas.
2. **Anonimato:** decimos que Bitcoin es un seudónimo, es decir, que en determinados casos sus transacciones pueden ser asociadas a sus poseedores con éxito. Se trata de dificultar este tipo de rastreo.
3. **Tipo de prueba:** el tipo de prueba de trabajo en Bitcoin, la Prueba de Trabajo, es criticada por su consumo energético. Han surgido propuestas que pretenden, o bien mitigar esta situación, o bien aprovechar el esfuerzo computacional con un segundo fin práctico.
4. **Ejecución de código:** Bitcoin dispone de un sistema simple de ejecución de código sin bucles. Esta restricción ha sido eliminada.

El conjunto de las blockchains que se pueden describir junto con sus tokens es enorme, si bien es verdad que existe una tendencia a trabajar sobre las blockchains públicas establecidas y a crear nuevas aplicaciones descentralizadas sobre sus protocolo, como se explica en la sección sobre inversión en criptomonedas. El tiempo irá seleccionando los proyectos que mejor se adapten a las necesidades del mercado. Muchos de ellos desaparecerán, pero los que encuentren su nicho, desarrollen e innoven, cambiarán nuestra forma de comprender las redes distribuidas para siempre.

El universo de las blockchains privadas

Las blockchains privadas o de acceso basado en permiso (llamadas por ello en inglés *permissioned*) son todas aquellas en las que el acceso ya no tiene por qué ser cien por cien público, sino que abren un abanico de posibilidades que va de lo parcialmente privado —como habilitar sólo acceso a ciertos procesos críticos, como puede ser un consenso, y a determinados participantes— hasta el acceso total. Entre unas y otras también pueden estar presentes construcciones híbridas entre las blockchains públicas y privadas.

Una red típicamente «pública» como Bitcoin o Ethereum podría usarse de manera «privada» si dicha red se despliega fuera de internet, por ejemplo en una intranet de empresa o una extranet con varias empresas. En este caso, el objetivo es usar la tecnología blockchain pública para el ámbito privado típicamente

empresarial, pero también se podría operar en un campo de interés público, pero controlado por una federación consensuada de grupos de interés u otros actores seleccionados. Es el caso de IPDB o Ripple.

Las blockchains privadas surgen con un propósito muy definido. En unos casos son iniciativas de compañías de consultoría blockchain que centran sus esfuerzos en «ayudar» a las empresas a entender el nuevo paradigma tecnológico que está por llegar, de modo que puedan anticiparse a cambios abruptos en sus mercados. En otros, son las propias grandes empresas las que toman la iniciativa de estudiar y desarrollar la filosofía blockchain, bien para justificar sus inversiones en tecnología, bien desde el íntimo convencimiento de que se trata de un elemento clave que asegura la optimización de muchos procedimientos actuales. Las que logren incorporar a su ADN la filosofía blockchain, prescindiendo del desfasado apéndice tecnológico de las actuales estructuras de BackOffice, serán las triunfadoras en el panorama empresarial que se avecina.

Todas estas iniciativas de blockchains privadas persiguen un objetivo práctico: pueden desarrollarse a nivel corporativo para una mayor eficiencia y optimización de los actuales procedimientos operativos; pueden crear un entorno de trabajo colaborativo entre compañías rivales de un mismo sector, que aporte beneficios a todos los participantes, y pueden también crear el futuro estándar para liderar la optimización en industrias asentadas o convertirse en referencia futura para el desarrollo de mercados aún por descubrir. El éxito en expandir estos protocolos privados podría transformarlos en las plataformas sobre las que se crearán los modelos de negocio que operarán la industria en el futuro.

Las industrias financiera y bancaria lideran el movimiento de las blockchains privadas y son la punta de lanza de una tendencia que también afecta a otros sectores, como seguros y reaseguros, telecomunicaciones o energía. En todos los casos imaginables podríamos asistir a la desintermediación de modelos de negocio tradicionales, con todos los retos que eso supone.

Soluciones propuestas desde las blockchains privadas

El nacimiento y consolidación de las blockchains privadas ha sido uno de los procesos más exitosos en los primeros años de vida de esta tecnología. Aunque al lector le pueda parecer que existe una rivalidad generalizada para imponer su modelo al resto, lo cierto es que en muchos casos se ha propiciado la relación, intercambio y colaboración entre distintos proyectos, siempre en busca de un beneficio común. De hecho, muchos inversores, especialmente del sector bancario, han invertido indistintamente en varios de estos modelos. No necesariamente tiene que triunfar y consolidarse una única blockchain global que integre todos los procesos y desarrolle todas las ideas y posibilidades, sino que distintas blockchains, con sus propias características y fines, pueden repartirse ese puesto hegemónico global o funcionar y colaborar entre ellas en perfecta armonía. Sólo el tiempo dirá qué tecnologías blockchain se impondrán sobre otras y cuáles son las aplicaciones que logran consolidarse y establecer un modelo de uso exitoso en sus industrias. Hyperledger, R3, Digital Assets Holdings, Chain, Symbiont, Mutichain, BigchainDB, Ripple, Interledger son algunas de esas soluciones.

Más información sobre las blockchains públicas y privadas en <libroblockchain.com/blockchain-publica/> y <libroblockchain.com/blockchain-privada/>.

Capítulo 13

Un mundo de muchas blockchains

Álex Preukschat, Álex Puig Pascual y Gonzalo Gómez Lardies

El internet de la información de la década de los noventa giró entre dos propuestas distintas: por un lado, el internet abierto, tal como hoy lo conocemos, y, por otro, el internet de pago cerrado propuesto por grandes empresas como AOL. El ecosistema blockchain, a diferencia del internet de la información, presentará una mayor diversidad, fruto de las necesidades de industrias, sectores y usuarios.

En los primeros años de las blockchains públicas era habitual oír hablar de todo tipo de nuevas criptomonedas, cada una con su propia blockchain, es decir, su cadena de bloques para almacenar secuencialmente las transacciones, su token y su protocolo. Esa moda duró aproximadamente de 2012 a 2015 y dio lugar a criptomonedas como healthcoin, peercoin, potcoin, solarcoin o spaincoin. En realidad, muchas de ellas no eran más que campañas de marketing que perseguían inflar el precio para que los pocos inversores iniciales soltaran sus criptomonedas en un mercado recalentado. Es lo que se llama un *pump and dump*. Por supuesto, también había proyectos serios, como litecoin, que experimentaba con otras funcionalidades dentro de su blockchain, o namecoin, la criptomoneda elegida por Blockstack para crear un internet descentralizado hasta que la necesidad de operar sobre blockchains más seguras la llevó a migrar su protocolo a Bitcoin.

A lo largo de 2016 se fue imponiendo la idea de que las blockchains públicas son las únicas que pueden prestar un servicio seguro. Además, se intuía que con el paso del tiempo se crearían puentes y conectores entre ellas y otras blockchains privadas, según fuéramos entendiendo en qué situaciones es más favorable el uso de una tecnología u otra. Independientemente de cuáles vayan a ser las blockchains que triunfen en el futuro, todo apunta a que se irá consolidando un ecosistema de blockchains públicas que generarán un nuevo reparto del valor en función de lo dinámicas que sean las capas superiores y sus

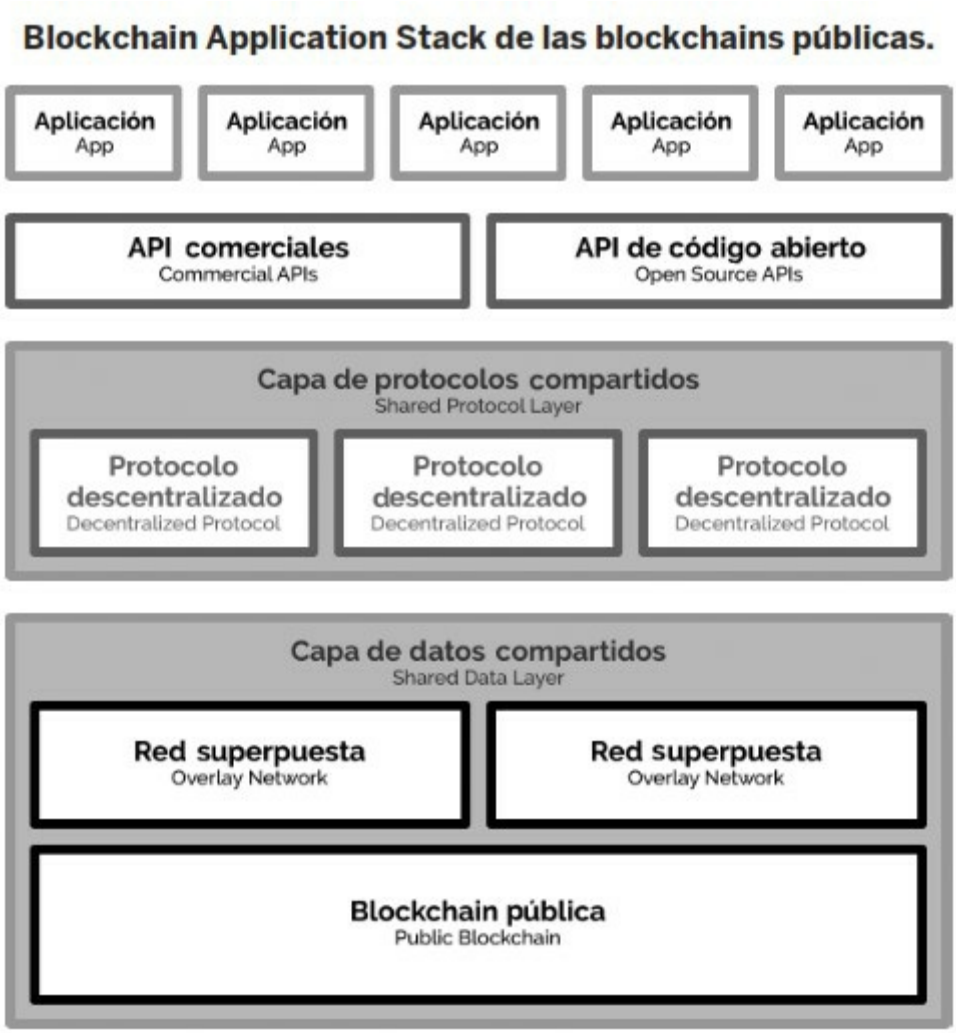
aplicaciones y modelos de uso reales. Es lo que Joel Monegro, de Union Square Ventures, llama «pila blockchain de aplicaciones» (Blockchain Application Stack, en inglés). En este modelo, las blockchains privadas podrían integrarse en diferentes niveles superiores.

El Blockchain Application Stack de las blockchains públicas

La arquitectura de las aplicaciones del internet del valor podría basarse en algo similar al Blockchain Application Stack y no tardar más de diez años en consolidarse. El esquema de la página siguiente puede servir para introducirnos en el mundo futuro que se nos plantea.

La idea básica es que todo lo que está dentro de los rectángulos grises se basa en código abierto y descentralizado. Nadie controla estas partes, que están a disposición de cualquier persona o empresa como infraestructura pública. Si tomamos Bitcoin como ejemplo, la cadena de bloques es la capa de datos compartidos (Shared Data Layer, en inglés). Según vamos subiendo en el Stack, cada capa se hace más fina y específica cuanto más arriba se encuentra. A continuación, veremos los distintos componentes con más detalle:

- **La capa de datos compartidos (Shared Data Layer):** esta capa se compone de una blockchain pública (por ejemplo, Bitcoin o Ethereum) y las Redes Superpuestas (Overlay Networks). Como su propio nombre indica, estas redes se superponen a la cadena de bloques de Bitcoin o Ethereum para realizar tareas que las redes de Bitcoin o Ethereum son incapaces de llevar a cabo, como una marca de tiempo o validar su trabajo. Counterparty, Factom y Sidechains de Blockstream son algunas Overlay Network que funcionan en la actualidad. Encima de ellas se pueden crear otros protocolos descentralizados con aplicaciones específicas.



Fuente: Joel Monegro/USV con adaptaciones de los autores.

- **Protocolos descentralizados (Decentralized protocols):** con la base de datos blockchain es posible desarrollar en código abierto protocolos descentralizados con datos incorporados por medio de Overlay Networks, con la confianza de que la validación y las transacciones o registros son veraces y no están controladas por una sola entidad. Estos protocolos descentralizados en la parte superior de la cadena de bloques tienen el potencial de deshacer ese valor añadido. La'Zooz y Synereo, como réplicas descentralizadas de Facebook y Twitter, u OpenBazaar de eBay, son algunos de estos protocolos.
- **Aplicaciones de código abierto y API comerciales (Open Source and Commercial APIs):** para el desarrollador medio, los protocolos son difíciles de construir en la parte superior de este esquema que estamos desarrollando. Sin embargo, se puede establecer una conexión con ellos a través de API. Algunos ejemplos de esta tendencia son la API de

Chain.com (un servicio comercial alojado en una blockchain privada) y Toshi de Coinbase (de código abierto, aunque Coinbase —un Exchange de bitcoins— abandonó el proyecto en diciembre de 2016).

- **Aplicaciones (Applications) blockchain:** ésta es la parte del esquema de acumulación de Monegro que se relaciona con el consumidor. Las aplicaciones construidas sobre esta arquitectura trabajan de manera muy similar a las que utilizamos en la actualidad. Para los consumidores, la diferencia es que, dado que se basan en protocolos descentralizados, son capaces de interactuar entre ellas y con diferentes aplicaciones de correo electrónico y carteras Bitcoin. Hay empresas como Circle que quieren innovar en los pagos entre pares y que, a efectos del consumidor, podrían considerarse un banco sin una relación aparente con la blockchain. En algunos casos estarán reguladas en aquellas jurisdicciones donde operan bajo la infraestructura clásica financiera, mientras que en otros utilizarán la blockchain para realizar pagos, por ejemplo, entre la India y Brasil. Circle y Coinbase en concreto trabajan con la blockchain de Bitcoin o Ethereum sin necesidad de recurrir a otras capas del Blockchain Stack, pero en el futuro otros proyectos podrán utilizar propuestas diferentes en las capas intermedias diseñadas. De este modo se facilitarán aplicaciones basadas en la blockchain y cada vez más descentralizadas. En este caso, el usuario final no tendría por qué ser consciente de que está utilizando una blockchain.

Desarrolladores, empresarios, emprendedores e inversores serán los protagonistas de la reubicación actual del valor en internet en esta nueva arquitectura descrita. Los beneficios de este modelo de acumulación los percibirá el usuario de muy distintas formas, bien como un notable ahorro en gastos asociados a la intermediación, bien con un nivel mayor en lo que se refiere a la protección de datos o la seguridad plena a la hora de operar en este mercado.

¿Qué pasa con el mundo de las blockchains privadas?

El modelo de las blockchains privadas ha recurrido a sistemas de financiación clásicos, sea a través de consorcios al efecto o de inversiones en empresas de capital riesgo. La razón no es otra que la confianza que le proporcionan los

modelos de monetización conocidos. Estas blockchains privadas, sin embargo, surgieron entre los años 2014 y 2015 con el propósito de crear el futuro estándar para sus respectivas industrias y reinventar sus modelos de negocio.

Independientemente de cuáles sean las soluciones de las blockchains privadas que se impongan en el futuro, una de las claves será cómo se comunicarán este ecosistema y el público. La blockchain pública cuenta con la ventaja de servir como registro de confianza y de sello temporal, pero es de esperar que las industrias y empresas quieran gestionar sus propias bases de datos descentralizadas independientemente de las blockchains públicas, bien para competir con ellas o simplemente para no depender de una comunidad de desarrolladores y mineros que podrían abandonar un desarrollo sin necesidad de dar explicaciones. En ese sentido, una de las cuestiones clave será la transferencia y compartición de datos entre blockchains públicas y privadas, y la forma de conectar ambos mundos. Con el tiempo veremos cómo se consolidan ambas tecnologías en sus ámbitos y cómo se crean y consolidan los puentes necesarios para compartir el intercambio de datos e información entre ellas.

Un nuevo sistema operativo de internet

Con todo lo visto hasta ahora podemos empezar a dibujar un esbozo de lo que el futuro nos depara. Si consideramos una blockchain como una base de datos en la cual todos los nodos comparten la misma información, no nos será difícil imaginar una blockchain como un solo ordenador universal compuesto por distintos discos duros que replican la información. El sistema operativo de este ordenador universal serían, por ejemplo, Ethereum o Hyperledger. De esta forma, los Smart Contracts de Ethereum o los Chain Codes de Hyperledger serían programas que podríamos instalar en este ordenador compartido con miles de usuarios, los cuales podrían acceder a estos programas mediante sus wallets o carteras digitales, es decir, de forma criptográficamente segura.

Si unimos a muchos de estos ordenadores universales (desde blockchains públicas a privadas), tendríamos la configuración de un nuevo internet distribuido y potencialmente mucho más potente y seguro que el que hoy conocemos.

Epílogo

Cerraremos estas páginas con un breve relato surgido de la imaginación de todos los autores y que nos traslada desde los años ochenta del pasado siglo hasta las primeras décadas del siglo XXI. Con él queremos dibujar el impacto que la blockchain podría tener sobre nuestras vidas en un futuro no tan lejano, y ello con un toque romántico y optimista. El relato se limita a reflejar 24 horas en la vida de un joven apasionado por las nuevas tecnologías desde su más tierna infancia, un nativo de la cadena de bloques a quien nos es imposible ponerle un nombre, pero que bien podría ser cualquiera de nosotros o, por qué no, tú mismo.

Una visión del mundo del futuro basado en la blockchain

Carlos Kuchkovsky Jiménez

En un año del futuro y en un municipio del extrarradio de una gran ciudad de España, el despertador suena a las 8 de la mañana en el dormitorio del joven protagonista de este relato. Abre los ojos y reconoce la melodía al momento. No en vano, ha sido seleccionada de antemano con la finalidad de ejercer un efecto estimulador con el que iniciar el día. Como un acto reflejo, murmura unas frases y activa el comando de voz. Es consciente de que ese acto va a desencadenar una serie de acontecimientos porque, de hecho, él mismo los ha programado. El primero, por más evidente, será que la alarma vuelva a sonar transcurridos quince minutos. A nuestro protagonista le encanta disfrutar de ese tiempo determinado que transcurre en un estado soñoliento. En esos quince minutos la cafetera se ha puesto en marcha, como sucede todos los días de la semana. Sin embargo, hoy es viernes, así que ninguna otra función se activa en la cocina. Los viernes se desayuna un café y un par de piezas de fruta que aguardan, sin más, en la nevera.

Hoy es un día especial. Nuestro protagonista cumple años y por eso permanece en la cama más despierto de lo habitual. Piensa en cosas recurrentes, pero la cena de esta noche con su novia consume prácticamente todos esos minutos. Es una persona de naturaleza profundamente optimista, y por eso, antes de levantarse siempre le embarga la misma sensación de ser muy afortunado. Su familia siempre le ha apoyado en sus decisiones, cuenta con buenos amigos, trabaja en lo que más le gusta y es feliz con su pareja.

Profesionalmente nuestro protagonista ha participado en numerosos desarrollos y proyectos tecnológicos, y actualmente es referente en uso y experimentación de las más sofisticadas propuestas innovadoras. Sus opiniones están muy bien consideradas y han contribuido al lanzamiento de algunos nuevos productos y aplicaciones tecnológicas de éxito. Mientras desayuna, accede a su dispositivo móvil. Se sorprende de las altas valoraciones recibidas —en cantidad y calidad— de una noticia tecnológica. Selecciona y programa la

audición de esa y otras mientras se ducha y arregla. Le gusta lo que ha escuchado, la presentación de un nuevo proyecto tecnológico de impresiones en 3D que facilita la producción local inteligente de bienes «a medida», listos para el consumidor final, minimizando costes de transporte a través del internet de las cosas (IoT). Decide apoyarlo e invertir con tokens, y así lo hace, enviando una preorden de compra que deberá confirmar en 24 horas. Luego se arrepiente y extiende el plazo 24 horas más. Si en los próximos dos días no cancela la orden, será accionista de la compañía. Una situación similar a las primeras visiones de una DAO, sólo que ahora perfectamente integrada en la Administración porque pagará los impuestos correspondientes de forma automatizada mediante los Smart Contracts integrados con la Hacienda Pública.

Siguiendo con la inercia, decide hacer también una donación a una ONG que anuncia una reestructuración completa de sus procedimientos actuales. La relación con los asociados se desarrollará a través de una blockchain privada, mientras que las relaciones con colaboradores, patrocinadores o instituciones se sustentarán en una pública. Esta nueva plataforma híbrida garantiza, al mismo tiempo, la privacidad de los usuarios y la transparencia en la gestión de los recursos. «Éste es el camino que seguir», piensa.

Después cierra la aplicación y se dispone a disfrutar de lo que se podría calificar de vicio inconfesable. Accede a su foro favorito, especializado en tecnología, a través de dos avatares distintos con los que gestiona su identidad digital. Uno lo utiliza de forma correcta e institucional, mientras que en el otro adopta posturas extremas y radicales. La absoluta garantía de privacidad y la tranquilidad de saber que difícilmente podrá desvelarse su identidad en este internet descentralizado le empujan a ser franco en ambos sentidos.

En algunas ocasiones, estos foros son un auténtico reducto de conocimiento e ideas originales, y de ahí su interés en leer y participar de forma activa desde posturas opuestas. Sus dos avatares tienen una alta consideración entre los usuarios y algunas veces son generosamente recompensados, con cantidades similares de tokens, puntos de reputación o «estrellas de fidelización» con algoritmos de valoración en tiempo real de activos. Una plataforma distribuida pública, que actúa como un gran mercado para anunciantes, patrocinadores, comerciantes y usuarios, acepta esas estrellas en el intercambio de bienes y servicios. Muchos de estos comercios asociados suelen también

reutilizarlas para recompensar al usuario por participar en encuestas de satisfacción o para pagar parte del salario a sus empleados o facturas a sus proveedores usuarios de la plataforma. Cumpliendo en parte con su visión que la identidad digital podría convertirse en el dinero del futuro. En el foro existe otra posibilidad de recompensa que nuestro protagonista evita intencionadamente: las valoraciones positivas también se pueden hacer notar en otros perfiles públicos centralizados, pero encuentra mayor satisfacción utilizando identidades descentralizadas y anónimas, y además cumple mejor con sus propósitos laborales. Así que, tal y como opera ahora mismo, lo considera el foro tecnológico casi perfecto.

Con el paso del tiempo —y el desarrollo de nuevas aplicaciones— nuestro protagonista ha logrado convertirse en una pequeña celebridad en su nicho de mercado. Una de sus ideas se implementó hace unos meses. Ahora es posible traducir simultáneamente las intervenciones de forma fidedigna a multitud de idiomas, abriéndose el foro, de forma literal, al talento esparcido por todo el mundo, independientemente de la lengua elegida para manifestarse. El uso de las identidades digitales descentralizadas permite además a todos los usuarios votar de forma transparente y comprobable, unas características éstas tan rompedoras que no pudieron ser obviadas mucho tiempo en otra parcela de la Administración pública. En las próximas elecciones municipales los ciudadanos volverán a votar en este nuevo escenario de innovación tecnológica.

Hoy utilizará parte de esas «estrellas token de fidelización» para pagar en el restaurante donde cenará con su novia. Y así lo dispone, utilizando inconscientemente, la cuenta del avatar formal.

Son ya las 9 y pico de la mañana y tiene que pensar en cómo llegar hasta el centro de la ciudad. Un desafortunado incidente con la compañía líder que gestiona desplazamientos comunes ha dañado seriamente su reputación. Cree haber sido víctima de una terrible confusión, así que ahora está inmerso en una disputa para aclarar la situación y que se le reintegre su anterior estatus. Sin embargo, es muy consciente de que está en «bancarrota reputacional» y es muy posible que ninguno de los coches conectados a la red quiera subirle a bordo por este malentendido. Quizá sea mejor claudicar y renunciar a un proceso que promete ser largo y tedioso. Y le malhumora sólo pensar en los esfuerzos que tendrá que invertir en limpiar su nombre. ¿Sería mejor aceptar la bancarrota y

empezar de cero? Resignado, piensa otras opciones. Siguiendo su filosofía de vida de afrontar los problemas como oportunidades, decide probar el servicio autónomo de autobús vecinal. Un análisis de los datos colectivos de su comunidad —concretamente patrones de desplazamiento— reveló el previsible éxito de un servicio de estas características.

En el ascensor se encuentra con su vecino, una persona mayor con la que mantiene una relación cordial. La típica pregunta de cortesía, «¿cómo está?», le da pie a un pequeño desahogo y manifiesta su indignación y lo injusto de su «bancarrota reputacional». El vecino, que gestiona la red eléctrica del edificio y forma parte del comité eléctrico del barrio, se compadece y ofrece su transporte como alternativa. No suele utilizar su coche pero al menos se obliga a sacarlo del garaje una vez al mes. Antes de arrancarlo, contratará un seguro obligatorio por las siguientes nueve horas y hasta el mes que viene. Pero hoy el vecino encuentra un inconveniente añadido. La prima ha subido ligeramente debido a las malas previsiones meteorológicas.

Nuestro protagonista agradece el ofrecimiento, pero lo rechaza amablemente. Ya ha contratado el servicio del autobús vecinal que, en apenas cinco minutos estará en el sitio indicado para recogerlo. Cancelaciones o minutos de retraso llevan aparejadas un recargo o descuento automático en el servicio, en función del infractor. ¡Y se han acabado las malas calificaciones reputacionales! Pero hoy no se registra ningún inconveniente y ya está cómodamente sentado en el autobús.

Pretende pasar el viaje escuchando música, pero antes de abrir la aplicación surge un recuerdo que posteriormente conduce a una reflexión. Localiza en su memoria la fecha aproximada del primer caso de éxito de este tipo de iniciativa de recopilación de datos colectivos y Crowdinvestment. Tuvo lugar en el ámbito de la industria farmacéutica por una nueva empresa creada de cero, nativa de blockchain. Otras grandes corporaciones también lo intentaron, pero sus grandes estructuras burocráticas imposibilitaron concretar nada similar.

La reflexión es recurrente. ¡Lástima no haber invertido algunos tokens en esa nueva empresa! La revalorización de sus acciones ha sido tan espectacular como la que experimentó Bitcoin en sus primeros años. Además, ahora podría estar usando ese servicio a un coste mucho más reducido que los nuevos

usuarios. De haberse dado de alta entonces, sus datos habrían formado parte del primer entrenamiento de los sistemas inteligentes de la empresa y, consecuentemente, hubieran generado mucho más valor que ahora. Sin embargo, se consuela reconociendo que entonces era un adolescente que apenas tenía recursos económicos para invertir. Pero de ahí, su imaginación le lleva a otra idea recurrente… «¿Sería posible replicar un éxito similar en un estado recién nacido, nativo de la blockchain? ¿Cómo sería?» Cuando desarrolle el concepto, ése será el próximo tema que publique en el foro, eso sí, bajo el anonimato del avatar revolucionario.

Accede a la aplicación musical. Tal y como la tiene configurada, presupuesta una cantidad mensual que se distribuye según sus preferencias. Así evita publicidad, cortes en las canciones y otros inconvenientes asociados. Las canciones que más escucha, más retribución se llevan. La verdad es que está encantado con esta aplicación y a pesar de tener que probar todas las propuestas del mercado, ésta es la más lograda porque integra todos los datos de los artistas a través de protocolos abiertos para que puedan ser recompensados de forma flexible.

Con esta aplicación descubrió nuevos talentos y, en alguna ocasión, ha ganado alguna apuesta, demostrando documentalmente, que en cierta forma, fue un promotor del grupo del que todo el mundo habla. Él gratificó la maqueta del primer disco de aquellos desconocidos. Sin embargo, hoy es su cumpleaños y no puede dejar de atender los mensajes de felicitación recibidos en la blockchain privada familiar.

Hace algunos años, cuando quedó prendado por este mundo, quiso desarrollar su propia blockchain privada. Necesitaba aprender y experimentar sobre el terreno. Le pareció una gran idea involucrar a personas de confianza que se responsabilizaran, de forma altruista, del mantenimiento de sus nodos. Así que recurrió a sus familiares. En unas Navidades, explicó su proyecto y acaparó cierta atención. Su generación mostró más entusiasmo que la anterior. Aunque el decidido apoyo de un miembro relevante de ésta, un hermano de su madre, fue definitivo para desarrollar la blockchain. Siempre sonríe cuando recuerda el acalorado disgusto de su tío cuando descubrió la difusión de unas fotos suyas en redes sociales. Normal, el documento gráfico era innegable y

retrataba a su tío con veinte años menos pero con cuarenta kilos de más. Aquello fue calificado de «insultante indiscreción» y la responsabilidad de aquella «infamia» recayó sobre todos sus sobrinos por igual.

Apenas transcurren tres minutos desde que se apea del autobús y llega a su cita. Las siguientes horas van a transcurrir en una sala de reuniones donde directivos, emprendedores, desarrolladores, abogados, técnicos e informáticos compartirán ideas, experiencias, normativas y espacio. Blockchain, inteligencia artificial, robótica, 3D, ordenadores cuánticos, automatización, IoT, M2M, plataformas en la nube, realidad virtual, ahorro de costes, seguridad, anonimato, transparencia, presente y futuro son las palabras más recurrentes. Pero a pesar de lo apasionante de la reunión, en una hora tiene una cita con su novia y ésa es la prioridad del día.

Llega un poco tarde y entra a trompicones en el restaurante. El lugar de encuentro no es una elección casual. Tenía muchas ganas de conocerlo porque se provee de verduras del huerto ecológico en el que invirtió hace años. Su novia lo espera sentada y con una copa en la mano. Su excusa es la habitual, un debate apasionado le hizo perder la noción del tiempo. Su novia sonríe. Le fascina la pasión de su pareja cuando habla de su trabajo, tanto, que compensa obviar cualquier reproche. Después empieza una velada privada que nada aporta a este relato.

Nuestro protagonista llega a su casa con un regalo. Cree saber de qué se trata pero, como ha prometido, sólo lo desenvuelve una vez metido en la cama. No se lo puede creer. Estaba convencido, pero le costaba creer que pudiera ser cierto. Su novia ha dado en el clavo. Entre sus manos tiene la primera edición de un libro de culto: *The code breakers*, de David Kahn. Lo leyó hace muchos, muchos años y, en cierta forma, actuó como detonador de un futuro distinto. ¡Y además está dedicado! Lee la cita que ha escrito su novia y se emociona. Apaga la luz y cierra los ojos, pero inevitablemente la cita regresa a su cabeza: «Feliz cumpleaños. Me ha costado mucho encontrarlo pero ha merecido la pena. Como sueles decir: “El recurso más sublime del que dispone cualquier persona es su capacidad para imaginar *cosas*”. Encontrarlo me ha llevado al límite de la mía. Un beso».

Agradecimientos

Álex Preukschat e Íñigo Molero Manglano

A todos los autores de este libro, por su desinteresada colaboración y en reconocimiento de esas horas robadas a su tiempo de ocio. Gracias por contribuir con vuestro talento y experiencia a enriquecer este libro.

A José Luis Várez Benegas por haber apoyado este proyecto desde la primera vez que le propusimos formar parte del mismo. De la misma forma —y para hacer una única mención en el texto a nuestra inmensa suerte—, hemos contado también con el apoyo incondicional de Daniel Díez García y Roberto Fernández Hergueta (everis), Gonzalo Gómez Lardies (Informática El Corte Inglés, IECISA) y Carlos Kuchkovsky Jiménez (BBVA). Un obligado agradecimiento que hacemos extensivo a sus organizaciones, por su involucración y apoyo en esta labor de difusión realizada por la comunidad blockchain española.

A Daniel y Gonzalo por compartir con nosotros las posibilidades de la blockchain en la banca y las aseguradoras, siendo Gonzalo clave para definir una visión de futuro de las tecnologías blockchain junto con Álex Puig Pascual.

A Dioni Nespral e Ignacio Madrid Benito (everis) por su contribución para poder entender el impacto de la tecnología blockchain en las industrias de salud y farmacéuticas, y el nuevo modelo energético.

A Christoph Steck y Eusebio Felguera Garrido (Telefónica) por ilustrarnos sobre las infinitas posibilidades de blockchain en el sector de las telecomunicaciones. Y a Óscar Lage Serrano (Tecnalia) por su argumentada explicación del previsible impacto de esta tecnología en la industria 4.0. y el futuro del voto electrónico.

Al experto en juego online Stefan Hamann, quien nos ha dado una muestra de los profundos cambios que se ciernen sobre el sector de la mano de la blockchain.

Al arquitecto doctor Stefan Junestrand, responsable de guiarnos por esa ciudad inteligente del futuro, evolucionada y optimizada por la tecnología.

A Roberto Díaz Bartolomé, que ha expuesto las nuevas posibilidades de gestión de las que podrían beneficiarse las pymes, y a Covadonga Fernández González, que nos ha mostrado el futuro que aguarda a los medios de comunicación en ese nuevo escenario del internet del valor.

A Adolfo Contreras Ruiz de Alda (Dejaki) y Félix Moreno de la Cova (Xapo) por esa brillante fundamentación sobre la transformación que experimentará el comercio electrónico, una lectura imprescindible y complementaria a nuestra visión de un nuevo internet basado en la blockchain. A Carlos Vivas Augier por enriquecer nuestra visión industrial y sectorial, y por sus explicaciones, concisas y amenas, sobre las posibilidades transversales de los Smart Contracts y las DAO. Una cuestión muy importante, enriquecida gracias a la labor clarificadora realizada por Cristina Carrascosa Cobos (Ecija), José Ramón Morales Cáceres (Garrigues), Xavier Foz Giralt y Joaquim Matinero Tor (Roca Junyent). Gracias por ese apunte legal tan necesario y complementario que resulta de obligada lectura. Cristina y Carlos, además, han aportado una perspectiva histórica del origen de los cypherpunks, imprescindible para entender el movimiento blockchain, un recorrido interesante aderezado con aportaciones clave realizadas por Víctor Escudero.

A Javier Molina Jordá (TokenCapital.com y El Confidencial.com) por esa muestra cuantitativa tan interesante de las posibilidades de la nueva economía de las criptomonedas, texto complementado con nuestra visión fundamental de este mercado.

En nuestro capítulo de tecnología hemos tenido el privilegio de contar con miembros veteranos y reconocidos de la comunidad blockchain española. Víctor Escudero Rubio interviene para explicar los principios del software libre; Jaime Núñez Miller revela magistralmente los principios básicos de la criptografía y el consenso, junto con Santiago Marquéz Solís, de quien hemos aprendido mucho sobre seguridad, igual que con Luis Carlos García sobre lo que es una transacción bitcoin o que con Manuel Polo Tolón y su visión del casi infinito abanico de posibilidades que suscitan las blockchains privadas. Son tantas, que una exposición más detallada de las mismas está disponible en nuestra web. Carlos Kuchkovsky cierra el libro con un relato en el que disecciona un día entero en la vida de un usuario en este futuro, tan descentralizado como posible.

Toda la labor recogida en el presente libro ha sido posible gracias al extraordinario equipo de Gestión 2000 (Grupo Planeta) que, de la mano de Roger Domingo, Daniel Lasheras Pancorbo y Carola Kunkel, nos ha facilitado todo el proceso. Para nosotros dos, Íñigo y Álex, ha sido un placer trabajar con este excelente equipo de profesionales del ecosistema blockchain y una especie de culminación a años de trabajo recogidos en una infinidad de artículos y análisis sobre esta tecnología y publicados en OroyFinanzas.com, junto con Elena Prieto Landaluce, y otros medios de comunicación.

También queremos agradecer al lector su interés y felicitarnos por que haya prevalecido en él esa mínima curiosidad necesaria para incorporarse a este nuevo universo tecnológico. Ése es nuestro deseo y ha sido nuestro reto: proporcionar una herramienta para que cualquier persona pueda aprender, comprender y formarse su propio criterio en torno al uso y posibilidades de la blockchain. Esperamos que la mayoría haya quedado prendada y comparta nuestra visión de este probable futuro. En ese caso, este libro sólo es un primer paso, pues el ecosistema blockchain evoluciona constantemente y casi tan importante es conocerlo, en detalle, como mantener cierta actualización de propuestas y desarrollos. Por eso queremos también poner, a su entera disposición, una página web complementaria con análisis más desarrollados de los temas que han conformado los capítulos de este libro, así como de otros nuevos que también serán de actualidad con el paso del tiempo y darán mucho de que hablar.

Confiamos que esta web que hemos creado al efecto, <www.libroblockchain.com>, pueda ser una especie de punto de encuentro entre lectores y autores, y que, entre todos, contribuyamos con opiniones, noticias o comentarios al enriquecimiento y difusión de la comunidad blockchain de España y el mundo hispano, como si se tratara de una especie de «nodos distribuidos» que comparten un mismo objetivo.

Dedicatorias personales

A mis padres y a mi madrina —ya octogenaria— por ser usuarios de esta tecnología, si bien, sospecho, más por cariño hacia el autor que por un descubrimiento personal o convencimiento propio. Lo mismo da, que les quiero

igual. Y, cómo no, a Álex por su determinación y capacidad de trabajo, de las que he sido testigo privilegiado, elementos imprescindibles para la materialización del presente libro.

ÍÑIGO MOLERO

A mi esposa e hijos por su apoyo en todas las aventuras en las que me embarco. Y a Íñigo y su extraordinaria capacidad literaria, con quien en los últimos años he creado un gran dúo que ha posibilitado este libro y otros muchos proyectos. Sin él, este trabajo tampoco habría sido posible.

ÁLEX PREUKSCHAT

Autores principales y coordinadores del libro

Álex Preukschat @AlexPreukschat

Desde 2012 es asesor de desarrollo estratégico, gestión de proyectos y formador de mandos en empresas multinacionales y startups dentro del ecosistema blockchain. A lo largo de su carrera ha trabajado en el sector financiero (Fintech) y turismo en facetas vinculadas a tecnología, marketing digital y desarrollo de negocio en distintos países. Asimismo, es autor y productor de la primera novela gráfica del mundo sobre Bitcoin (BitcoinComic.org) y de juegos móviles inspirados en el mundo de las criptomonedas (MoneyFunGames.com). Estudió en la Universidad Pontificia Comillas-ICADE E-4 de Madrid (España) y en la ESB Business School de Reutlingen (Alemania).

Carlos Kuchkovsky Jiménez @MisterKUCH

Ingeniero informático apasionado por la continua transformación social propiciada por la tecnología y por la nueva economía P2P. Ha trabajado como desarrollador dentro de la industria del juego y, actualmente en el BBVA, trabaja para mejorar la interacción persona-finanzas dentro de la banca. Cofundador y coorganizador de los grupos de interés APIHour y El Mundo Descentralizado, desarrolla también otros proyectos más personales como L8SmartLight.

Gonzalo Gómez Lardies @gglardies

Con más de diez años de experiencia en el área de consultoría estratégica y de negocio, es responsable de la estrategia de innovación y oferta digital para el sector financiero (Banca&Seguros) en Informática El Corte Inglés. Es ingeniero informático por la Universidad Politécnica de Madrid, donde realizó un máster en consultoría y gestión de empresas. En 2016 obtuvo el mejor expediente académico de su promoción en el programa directivo «Banca digital: innovación y tecnología financiera» que imparte el Instituto de Estudios Bursátiles.

Daniel Díez García @Danicellero

Emprendedor desde fecha temprana en temas relacionados con Bitcoin y blockchain, ha desempeñado el cargo de director de estrategia y desarrollo de negocio en Bit2Me, la primera aplicación que conectó a la red ATM tradicional, galardonada como mejor startup de España en 2015. Es también cofundador de la primera consultora española de blockchain, Furai. Actualmente trabaja como responsable de blockchain para EMEA y Latam en everis, desde donde coordina la estrategia tecnológica multisector.

Íñigo Molero Manglano @Imolman

Licenciado en Derecho y Periodismo, es consultor en comunicación. Durante muchos años ha estado ligado al tercer sector como dircom de ONG y de Redes de Asociaciones Internacionales. Ha participado también en proyectos auspiciados por la Comisión Europea, encabezando las tareas de comunicación. En la actualidad es colaborador y analista en OroyFinanzas. com y asesor en comunicación de tecnología blockchain.

Autores colaboradores del libro

José Luis Várez Benegas @BlockLiftHQ

Emprendedor, inversor y banquero involucrado en innovación tecnológica a lo largo de toda su carrera. Fundador de Blocklift y otros proyectos relacionados con la blockchain, es un firme defensor de la tecnología blockchain, de la que afirma que llegará a ser tan importante y disruptiva como en su momento lo fue internet.

Eusebio Felguera Garrido @EusebioFelguera

Ingeniero de Telecomunicaciones y máster en Negocio de las Telecomunicaciones, apasionado de la innovación y los nuevos modelos de negocio del mundo móvil, desarrolla su actividad actual como gerente en Políticas Públicas e Internet de Telefónica. Experto en redes móviles y negocios mayoristas, formó parte de la startup móvil Medí Telecom, segunda operadora de Marruecos. Ha sido gerente de regulación corporativa en Telefónica y tiene una dilatada experiencia en entornos internacionales, especialmente en la GSMA.

Christoph Steck @christophsteck

Abogado, MBA del IE Business School y profesor asociado en la School of Human Science and Technology del IE University, actualmente es director de Public Policy & Internet de Telefónica, cargo desde el que se ocupa de la estrategia y el posicionamiento de la compañía en internet. Es también vicepresidente del grupo de economía digital de la Cámara de Comercio Internacional (ICC), copresidente del consejo de miembros organizativos de la Internet Society (OMAC) y presidente del grupo de gobernanza de internet de ETNO.

Ignacio Madrid Benito @ imadridbenito

Ingeniero industrial del ICAI, experto en tecnología e innovación en el sector energético, ha trabajado con las principales compañías eléctricas, tanto en España como a nivel internacional, siempre sobre nuevos modelos de negocio y de colaboración con startups. Actualmente es director en el área digital de everis y responsable del área de Utilities, donde propone aplicaciones concretas de la blockchain a los principales agentes del sector.

Óscar Lage Serrano @Oscar_Lage

Responsable de Ciberseguridad en Tecnalia, cuenta con una amplia experiencia en la aplicación de ciberseguridad y algoritmos criptográficos en diferentes dominios (medios de pago, Smart Grid, industria 4.0, etc.). Participa habitualmente en grupos de opinión, estandarización y asesoramiento en ciberseguridad. Además, ha sido promotor de varias startups relacionadas con la ciberseguridad y colabora con varias aceleradoras.

Dioni Nespral @DioniNespral

Digital Shifter, ADE por la Universidad Antonio de Nebrija y EXMBA por el IE Business School, actualmente es director digital en everis, desde donde acompaña a las compañías hacia la construcción de nuevos modelos digitales de éxito. Su experiencia incluye la realización de proyectos digitales relevantes para el sector farmacéutico y grandes organizaciones públicas. Conferenciante, escritor y formador, dirigió la realización del libro *El futuro es tuyo*, en el que participaron 120 autores. Es uno de los coautores del libro *Inprendedores*, editado por la EOI y la Fundación Telefónica.

Roberto Díaz Bartolomé @robertodzbt

Entusiasta de la tecnología blockchain desde sus inicios, fundó su primera startup a los veintitrés años. Después fue responsable de marketing y crecimiento en Bit2Me (primera app en conectar Bitcoin con la red tradicional de cajeros, y startup del año 2015 en la categoría de tracción por Caixabank),

cofundador de Furai (primera consultora española de blockchain) y coautor del curso «Blockchain Toolkit». Actualmente es responsable de crecimiento en anfix.com.

Stefan Hamann @stef_hamann

MBA en el Massachusetts Institute of TechnologyMIT Sloan, en la actualidad asesora en Desarrollo de Negocio, Ventas, M&A y Business Intelligence a empresas multinacionales y startups vinculadas al sector del juego. En esta misma industria ha trabajado como gerente de empresas líderes del mercado como 888.com y Paddy Power.

Covadonga Fernández González @CuadraLab

Periodista de formación, ha desarrollado su labor profesional en Grupo Z, *ABC*, Canal de Isabel II y Telemadrid, televisión de la que fue presidenta. Consultora de comunicación, es la fundadora de OléChain, «el sitio para participar en los procesos que están cambiando el mundo». En la actualidad, colabora con la agencia EFE y escribe sobre blockchain en *CriptoNoticias*, además de ser profesora de comunicación en la Universidad de Alcalá de Henares.

Roberto Fernández Hergueta @rfhergueta

Digital Thinker & Maker, rulebreaker y matemático, es director digital en everis y responsable de la práctica de blockchain dentro del desarrollo de nuevos modelos de negocio digitales. Es también colaborador de escuelas de negocio como Imperial College Business School y ESADE, donde imparte clases sobre los nuevos modelos de marketing del siglo XXI.

Stefan Junestrand @sjunestrand

Arquitecto y especialista en edificios y ciudades inteligentes, trabaja como director general de Grupo Tecma Red, una empresa líder en información, comunicación y generación de conocimiento sobre energía, sostenibilidad y nuevas tecnologías en la edificación y la ciudad.

Adolfo Contreras Ruiz de Alda @acrual

Dirige Dejaki Soluciones, empresa dedicada a crear, diseñar, desarrollar y comercializar soluciones propias y para terceros basadas en múltiples tecnologías, así como a la consultoría en el desarrollo de negocios empresariales.

Félix Moreno de la Cova @flix1

Trader de bolsa, materias primas y divisas, es socio fundador y gestor de carteras en RockFlower Trading. Lleva involucrado en el mundo de Bitcoin desde 2011. Actualmente ejerce como CFO en Xapo.

Carlos Vivas Augier @cvivasa

Ingeniero informático, máster en tecnología de la información y doctor en economía interesado en el impacto económico de la tecnología en las empresas y la sociedad, hoy dirige Opinno Academy, desde la que se desarrollan habilidades técnicas en tecnologías emergentes como la blockchain. Ha fundado dos startups en el ámbito de las tecnologías digitales y es cofundador de Celera, una entidad sin ánimo de lucro que se dedica a fomentar el talento de personas del mundo de la ciencia, la tecnología y el emprendimiento.

Javier Molina Jordá @Molina_Jorda

Economista y máster en Mercados Financieros, ha sido responsable de productos cotizados y director de productos estructurados para banca privada en Société Générale. Asimismo, ha estado al mando de la mesa de Equity

Derivatives para América Latina en Société Générale, en Nueva York. Actualmente es analista independiente y colaborador económico en *El Confidencial* y TokenCapital.com.

Xavier Foz Giralt @XaviFoz

Es socio del área de derecho bancario y financiero de Roca Junyent y profesor asociado de la Universidad Pompeu Fabra de Barcelona. Asesora a empresas del sector Fintech y ha sido colaborador del Blockchain Space, el primer programa de aceleración de proyectos blockchain en España.

Joaquim Matinero Tor

Es abogado del área de derecho bancario y financiero de Roca Junyent. Asesora a empresas del sector Fintech y ha sido colaborador del Blockchain Space, el primer programa de aceleración de proyectos blockchain en España.

José Ramón Morales Cáceres

Abogado especializado en Derecho Mercantil y Derecho de las Tecnologías de la Información, es responsable de la industria de Tecnología & Outsourcing de Garrigues, dedicado a aspectos corporativos, transaccionales y regulatorios de proyectos tecnológicos y digitales.

Cristina Carrascosa Cobos @CarrascosaCris_

Abogada especializada en Derecho de Empresa, graduada del LLMM por el IE Law School. En la actualidad es asociada sénior del departamento de Tecnología de la Información, Propiedad Intelectual e Industrial y Protección de Datos en ECIJA. Interesada en blockchain y Smart Contracts desde su perspectiva legal, presta asesoramiento a proyectos relacionados con la implantación de esta tecnología.

Jaime Núñez Miller @jaimenm

Es socio fundador de Bankabit, una entidad dedicada al desarrollo de instrumentos para el sector de las criptodivisas, y de Zentank, una consultora de comunicación estratégica y desarrollo de servicios web. A lo largo de sus más de treinta años de carrera profesional ha creado y asesorado a varias empresas de tecnología, comunicación y comercio electrónico. Es miembro de la comunidad Bitcoin desde sus inicios.

Víctor Escudero Rubio @VEscudero

Experto en ciberseguridad, actualmente desarrolla sus funciones como arquitecto de seguridad para una importante entidad bancaria de ámbito nacional. Apasionado por el software libre, desde que conoció Bitcoin en sus orígenes participa activamente en la difusión del conocimiento sobre protocolos basados en las blockchains.

Santiago Márquez Solís @smarquezsolis

Project manager en Software AG, desarrolla aplicaciones de gestión económica para la TGSS. Es fundador de la empresa de videojuegos z-games y autor de los libros *Bitcoin. ¿Jaque mate al sistema financiero*? y *Bitcoin: Guía completa de la moneda del futuro*.

Luis Carlos García González

Licenciado en Ciencias Físicas por la UNED, administrador de sistemas GNU/Linux, defensor y promotor de aplicaciones libres e interesado en criptografía, llegó a Bitcoin en 2012. Trabaja para Renfe Operadora.

Manuel Polo Tolón @mrmx

Arquitecto de software, descubrió Bitcoin en 2010 y desde verano de 2011 trabaja como minero con GPU/ASIC. En 2013 desarrolló una bolsa de intercambio y puso en marcha el procesador de pagos Pagobit. Actualmente se dedica a la innovación con la blockchain dentro de everis para expandir su uso entre clientes de banca y otros sectores.

Alex Puig Pascual @alexpuig

Consultor de innovación y emprendedor tecnológico, especializado en cómo la tecnología puede impactar en la economía. Es el fundador y organizador de Digital Currency Summit, ciclo de conferencias sobre el impacto de las criptomonedas y la tecnología blockchain en sectores como la banca, los seguros o la energía.

Notas

1. Bitcoin.org: Bitcoin: A Peer-to-Peer Electronic Cash System, noviembre de 2008.

2. OroyFinanzas.com: Token Bitcoin: ¿Qué es un token en Bitcoin?, octubre de 2014.

3. OroyFinanzas.com: Diferencias entre las cadenas de bloques (blockchain) públicas y cadenas de bloques privadas, octubre de 2015.

4. <https://bitcoin.org/bitcoin.pdf>.

5. Directiva que cambia las normas europeas del seguro para reforzar esta industria y proporcionar mejores productos aseguradores a los ciudadanos. En España, entró en vigor el 1 de enero de 2016. El objetivo principal consiste en mejorar el control y medición de los riesgos (de mercado, operacionales, de crédito y de liquidez) a los que están expuestos las aseguradoras. Fuente: www.unespa.es/frontend/unespa/Que-Es-Solvencia-II-vn2783-vst16>.

6. Nuestro agradecimiento a la consultora Sita Schwenzer por sus aportaciones sobre el sector asegurador y blockchain en Europa.

7. <https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf>.

8. <https://fdd.etherisc.com>.

9. <www.pubpub.org/pub/medrec>.

10. <www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive>.

11. <www.cryptocoinsnews.com/self-driving-vehicles-and-smart-contracts-blockchain>.

12. <https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf>.

13. <https://filament.com>.

14. <http://www.energy.siemens.com/hq/pool/hq/energy-topics/publications/living-energy/11-12-2014/02_A%20Decentralized%20World-11.pdf>.

15. <https://techcrunch.com/2016/12/13/electron-is-trying-to-sell-a-blockchain-makeover-to-the-uks-energy-sector/>.

16. <http://news.usa.siemens.biz/press-release/energy-management/siemens-and-us-startup-lo3-energy-collaborate-blockchain-microgrids>.

17. <www.cryptocoinsnews.com/solarcoin-rewards-solar-energy-users-allow-users-trade-unused-electricity/>.

18. <https://www.powerpeers.nl/>.

19. <https://btcmanager.com/news/business/blockchain-to-power-renewable-energy-and-batteries/>.

20. <http://enerchain.ponton.de/index.php/13-ponton-develops-a-smart-market-for-german-flexibility-providers>.

21. <http://www.ibtimes.co.uk/rwe-slock-it-electric-cars-using-ethereum-wallets-can-recharge-by-induction-traffic-lights-1545220>.

22. <http://www.industrialdataspace.de/>.

23. <https://www.owasp.org/index.php/OWASP_Internet_of_ThingsProject#tab=IoT_Vulnerabilities>.

24. <https://time.tno.nl/media/7419/factories_4_0_egbertjan_sol.pdf>.

25. Nuestro agradecimiento a la doctora Laura López Fuertes y al doctor Andrés Konig Merediz por sus aportaciones sobre el sector farmacéutico.

26. Según un estudio de Health Research Funding Organisation, entre el 10% y el 30% de los medicamentos vendidos en países en vías de desarrollo son falsos.

27. <Blockverify.io>.

28. <isolve.io>.

29. <blockrx.com>.

30. <blockchainhealth.co>.

31. <guardtime.com>.

32. <pokitdok.com>.

33. <http://www.egba.eu/facts-and-figures/market-reality/>.

34. <https://tierion.com/>.

35. <https://www.satoshidice.com>.

36. <http://fintechnews.ch/blockchain_bitcoin/transparent-gambling-blockchain-gambling-industry-how-blockchain-can-make-it-more-transparent/3844/>.

37. <https://www.augur.net/; https://www.gamcrowd.com/news/article/blockchain-case-study-prediction-markets-and-augur>.

38. <http://www.quanta.im/>.

39. <https://virtue.poker/>.

40. <steemit.com>.

41. <http://politica.elpais.com/politica/2015/12/16/actualidad/1450287352_341538.html>.

42. <Hyperledger.org>.

43. <Satoshipay.io/>.

44. <https://pagefair.com>.

45. <https://launch.blendle.com/>.

46. <http://www.unonimity.com>.

47. <https://www.brave.com>.

48. <https://www.svdj.nl>.

49. Según el barómetro CIS (Centro Investigaciones Sociológicas) de diciembre de 2016, la segunda preocupación de los españoles es la corrupción y el fraude; la cuarta, los partidos políticos y la política: <http://datos.cis.es/pdf/Es3162mar_A.pdf>.

50. Metavalores blockchain (trazabilidad, descentralización, confianza y transparencia), unidos al potencial de los contratos inteligentes y agentes autónomos.

51. <https://followmyvote.com/>.

52. Desarrollado por el Departamento de Trabajo y Pensiones y el banco Barclays.

53. Según el anuncio de la Oficina de Medios de Comunicación de Dubái en octubre de 2016.

54. <http://www.jasonkitcat.com/>.

55. <https://thevotingnews.com/tag/bruce-schneier/>.

56. Castells, M., *La ciudad informacional*, Madrid, Alianza Editorial (1995).

57. La ciudad de Yinchuan (China) ha apostado por crear una ciudad inteligente basada en la blockchain: <http://edition.cnn.com/2016/10/10/asia/yinchuan-smart-city-future>.

58. <http://web.mit.edu/cron/project/CUPUM2015/proceedings/Content/pss/291_li_h.pdf>.

59. <http://smartcities.gov.in>.

60. <https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>.

61. <http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-nacional-ciudades-inteligentes.aspx>.

62. <https://www.smartnation.sg>.

63. <https://www.fiware.org>.

64. <https://account.lab.fiware.org>.

65. <http://www.fiware.in>.

66. David, N., Justice, J., McNutt, J.: *Transforming City Governments for Successful Smart Cities*, Springer International Publishing, Londres (2015).

67. Las dos principales tecnologías son el GIS (Sistema de Información Geográfica) y el BIM (Modelado de Información de Edificios).

68. Sistemas de este tipo existen actualmente en cientos de ciudades, como Santiago de Chile, Dubái, Toronto, Tel Aviv, Oslo, Milán, Londres y Estocolmo.

69. Este sistema se utiliza en muchas ciudades españolas, como Madrid, Barcelona y Sevilla.

70. Para crear un mejor flujo de las personas y aumentar la accesibilidad, en un cada vez mayor número de ciudades ya no se puede pagar en efectivo directamente en el transporte público, y en varias ciudades se está experimentando con pago por NFC, o incluso con reconocimiento facial basado en la blockchain, como en Yinchuan (China).

71. La'Zooz, por ejemplo, es un servicio de transporte compartido basado en la blockchain: <http://lazooz.org>.

72. Por ejemplo, la Estrategia Europea de Economía Circular: <http://ec.europa.eu/priorities/jobs-growth-and-investment/towards-circular-economy_en>.

73. <https://www.boe.es/doue/2010/153/L00013-00035.pdf>.

74. La iniciativa Brooklyn Microgrid genera y distribuye energía solar entre sus participantes gracias a un sistema de gestión basado en la blockchain: <http://brooklynmicrogrid.com/>.

75. Más información en <BitcoinComic.org>.

76. <http://www.forbes.com/sites/georgehoward/2015/06/05/bitcoin-and-the-arts-and-interview-with-artist-and-composer-zoe-keating/2/>.

77. <http://www.forbes.com/sites/georgehoward/2015/07/28/imogen-heap-gets-specific-about-mycelia-a-fair-trade-music-business-inspired-by-blockchain/>.

78. <http://www.forbes.com/sites/georgehoward/2015/07/28/imogen-heap-gets-specific-about-mycelia-a-fair-trade-music-business-inspired-by-blockchain/>.

79. <https://blog.ujomusic.com/building-ujo-1-from-the-technical-underground-to-the-future-a39e825612ef>.

80. <https://medium.com/ipdb-blog/a-decentralized-content-registry-for-the-decentralized-web-99cf1335291f>.

81. <https://www.pixelrockstar.com/open-letter-mediachain-search-photos/>.

82. Algunos ejemplos son: <Resonate.is>, <Bittunes.co.uk>, <Ujomusic.com>, <Peertracks.com>, <dotblockchainmusic.com>.

83. Por ejemplo: <Ascribe.io>, <Monegraph.com>, <Jaak.io>, <Alexandria.io> o <Yours.org>.

84. <http://arstechnica.com/security/2015/04/ddos-attacks-that-crippled-github-linked-to-great-firewall-of-china>/.

85. <http://arstechnica.com/security/2013/01/turkish-government-agency-spoofed-google-certificate-accidentally/>.

86. <http://www.businessinsider.com/hacker-social-engineer-2016-2>.

87. Más información en <https://ipfs.io/>.

88. <https://blockstack.org/virtualchain.pdf>.

89. Werner Vogel, CTO de Amazon.

90. Mencionado por Ryan Shea en <https://hackernoon.com/fixing-the-internet-7f6a57da5826>.

91. <https://www.statista.com/statistics/261245/b2c-e-commerce-sales-world-wide/>.

92. BitMarkets en <https://voluntary.net/bitmarkets/> es otro protocolo de e-commerce descentralizado.

93. <https://coinmarketcap.com/all/views/all/>.

94. Este identificador único de una billetera bitcoin sería como el número de cuenta del comercio.

95. <http://www.coindesk.com/research/state-bitcoin-blockchain-2016/>.

96. <https://blog.bitpay.com/bitcoin-a-new-global-economy/>.

97. <https://cointelegraph.com/news/roman-vacation-bitcoin-style-how-to-book-italian-taxis-with-crypto>.

98. <http://www.coindesk.com/point-of-sale-giant-ingenico-rolls-out-world-wide-bitcoin-payments/>.

99. <http://www.siliconbeat.com/2016/12/30/airbnb-users-want-2017-airbnbsmars/>.

100. <http://www.coindesk.com/uber-argentina-bitcoin-partnership/>.

101. Por ejemplo Bizum o Twyp.

102. Nota curiosa, el comando usado es *Suicide* en uno de los lenguajes de programación (*Solidity*).

103. <http://journals.uic.edu/ojs/index.php/fm/article/view/548/469>.

104. <https://github.com/DavidJohnstonCEO/DecentralizedApplications>.

105. Una blockchain de un nodo puede ser pública, pero no es descentralizada.

106. Se habla de la Web 2.0 (Social) y Web 3.0 (Semántica). Quizá Dapps sea la Web 4.0.

107. <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>.

108. Joel Monegro/USV: <http://www.usv.com/blog/fat-protocols>.

109. <http://www.coindesk.com/a16z-usv-invest-10-million-blockchain-token-trading-polychain-capital/>.

110. Artículo 1 de la Ley 35/2003 de 4 de noviembre de Instituciones de Inversión Colectiva.

111. En el caso de TheDAO, eran tokens específicos para TheDAO.

112.
<https://www.reddit.com/r/ethereum/comments/4auw6z/new_slockit_milestone_reached_the_dao_whitepaper

113. Puede considerarse como una sub DAO, similar a lo que sería una entidad matriz, y una filial que cuelga de la misma, pero sin los efectos societarios que tienen éstas en nuestro derecho.

114. Creador de b-money al cual hace referencia el white paper de Satoshi.

115. Nombre en clave de uno de los miembros de Chanology, proyecto impulsado por Anonymous que aparece en el Documental *We are Legion*.

116. Foro en el que se compartían memes con tono jocoso.

117. <https://xapo.com>.

118. <https://medium.com/shekel-magazine/odd-bedfellows-the-strange-history-of-visa-and-how-it-relates-bitcoin-101a93507c17>.

119. <http://nirakara.org/>.

120. <https://opensource.org/licenses/alphabetical>.

121. Satoshi Nakamoto, «Bitcoin P2P e-cash paper», 31 de octubre de 2008.

122. Por «cliente» se entiende una forma con la que se nombra a determinadas aplicaciones informáticas que hacen uso de un recurso remoto que se genera en otro ordenador conocido como «servidor». En las redes entre pares o P2P las aplicaciones que ejecutan sus usuarios son a la vez clientes y servidores, y hacen de nodos en la red (puntos a los que se conectan otros usuarios como clientes para recibir el servicio definido en el protocolo que establece las reglas que siguen los ordenadores constituyentes de ese tipo de red).

123. El Sistema de Nombres de Dominio (DNS) es un sistema descentralizado de nomenclatura que asocia diversa información a los dispositivos conectados a redes IP y traduce los nombres de dominios a direcciones numéricas.

124. «The Times 03/enero/2009 ministro de Hacienda al borde del segundo rescate para bancos». La frase se refiere a una nota de prensa de la misma fecha que hace alusión a quien entonces era el ministro de Hacienda del Reino Unido (Chancellor of the Exchequer), Alistair Darling.

125. Al proceso de generación de nuevos bloques que formarán parte de la cadena se le conoce como «minería».

126. El número de confirmaciones es simplemente el número de bloques que cuelgan del bloque que contiene la transacción, incluido éste. Cada nuevo bloque añade una nueva confirmación a todas las transacciones contenidas en la cadena, por tanto, el número de confirmaciones no deja nunca de crecer.

127. Es la primera transacción del bloque y está presente en todos ellos. Puesto que esta transacción especial no tiene entradas, el número saldo reflejado en ella supone la emisión de nuevos bitcoins. A su vez, sirve como mecanismo para distribuir la nuevas monedas acuñadas. La dirección destinataria es añadida por el nodo al resolver el bloque y pasan a ser controladas por su propietario.

128. Se trata de un servicio web que facilita la búsqueda de información en la blockchain en un formato legible.

Blockchain. La revolución industrial de internet

Alexander Preukschat, Carlos Kuchkovsky, Gonzalo Gómez Lardies, Daniel Díez García e Iñigo Molero

Gestión 2000 es un sello editorial de Centro Libros PAPF, S. L. U.

Grupo Planeta, Av. Diagonal, 662-664, 08034 Barcelona (España)

Primera edición en libro electrónico (epub): mayo de 2017

ISBN: 978-84-9875-448-3 (epub)

Conversión a libro electrónico: Newcomlab, S. L. L.