LA *BLOCKCHAIN*: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS

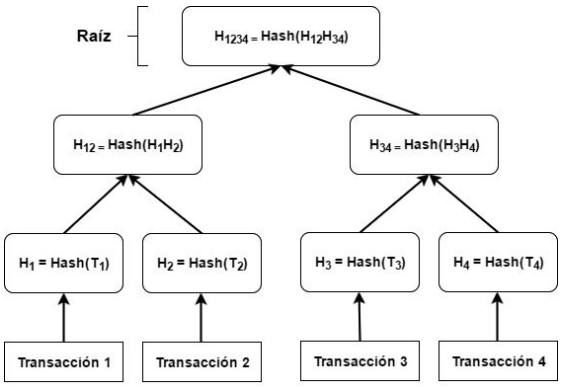
CARLOS DOLADER RETAMAL
JOAN BEL ROIG
JOSE LUÍS MUÑOZ TAPIA
Universitat Politécnica de Catalunya

Desde su publicación en 2009, *bitcoin* ha pasado de ser una propuesta de sistema alternativo de pagos, a la cripto-moneda más exitosa hasta el momento, con una nada despreciable capitalización que llega a los dieciséis mil millones de dólares (Bitcoin Price Index, 2017). Siguiendo su ejemplo, ha florecido un amplio ecosistema de monedas electrónicas paralelas y aplicaciones que comparten parte del éxito de bitcoin. Todas ellas tienen algo en común: la blockchain. La «cadena de bloques» o blockchain vio la luz en 2008 con la publicación de un artículo (Nakamoto, 2008) donde se explicaba el protocolo que usa actualmente bitcoin. Este nuevo concepto formaba parte de un sistema para procesar transacciones electrónicas de forma que no fuera necesaria una autoridad central o un sistema de fideicomiso (*escrow*). A principios de 2009 se publicó el primer cliente bitcoin, de código abierto, con el que empezó a funcionar la creación de bitcoins y la base de datos pública e inmutable con las transacciones, conocida como «ledger» (libro de registros). La tecnología para implementar este libro de registros fue la blockchain.

Aunque originalmente la cadena de bloques fue creada para almacenar el historial de transacciones del *bitcoin*, con el paso del tiempo se le ha visto gran potencial para ser aplicada en otros ámbitos debido a las propiedades que ofrece. La *blockchain* proporciona una base de datos distribuida inmutable basada en una secuencia creciente de bloques. Estos bloques, al ser públicos, conforman un sistema abierto que potencia la confianza en base a la transparencia y a la solidez de la técnica de construcción de la *blockchain*. El sistema, aunque es abierto, es también semi-anónimo: los usuarios se identifican con claves públicas (pseudónimos), no con sus identidades reales. En este contexto, podemos encontrar una primera relación entre la *blockchain* y *big data*: la necesidad de asegurar un entorno de pagos legal y libre de fraudes ha llevado al desarrollo de herramientas de análisis basadas en técnicas de *big data* para procesar la gran cantidad de datos representados en la *blockchain* (Ron, 2013, April) y (Reid, 2013). Por tanto, el anterior, es un posible caso de uso de *big data* para mejorar los procesos de inserción de datos en la *blockchain*.

Sin embargo, también podemos encontrar casos de uso a la inversa, es decir, casos donde se utiliza la tecnología *blockchain* para mejorar procesos en el entorno *big data*. En este sentido, la *blockchain* puede proporcionar robustez, seguridad, transparencia y escalabilidad a grandes sistemas de datos, lo que permite hacer frente a un amplio abanico de amenazas. Esto incluiría desde fugas de infor-

FIGURA 1
ÁRBOL DE *HASH* DE MERKLE



Fuente: Elaboración propia

mación a manipulación maliciosa del contenido. Mediante la *blockchain*, estas amenazas pueden combatirse trazando individualmente todas las acciones realizadas sobre los datos, resultando en una auditoría constante. Finalmente, otro caso de uso para la *blockchain* se podría dar en el ámbito del Internet de las cosas. Un ejemplo es la distribución segura y fiable de *firmware* a dispositivos IoT mediante un sistema de archivos *peer-to-peer* sobre *blockchain* (Benet, 2014). En este caso de uso, se podría utilizar la *blockchain* para almacenar actualizaciones de *firmware* de una forma descentralizada y segura (Christidis, 2016).

Una vez introducido el contexto de la *blockchain*, el resto del artículo describe el funcionamiento de esta tecnología en mayor detalle y proporciona una descripción más amplia sobre posibles aplicaciones de la misma en diversos ámbitos.

FUNDAMENTOS TÉCNICOS DE LA CADENA DE BLOQUES

Descripción básica

La cadena de bloques es una base de datos que puede ser compartida por una gran cantidad de usuarios en forma *peer-to-peer* y que permite almacenar información de forma inmutable y ordenada. En el caso de *bitcoin*, la información añadida a la *blockchain* es pública y puede ser consultada en cualquier momento por cualquier usuario de la red. La información solo puede ser añadida a la cadena de bloques si existe un acuerdo entre la mayoría de las partes. Transcurrido un cierto tiempo, se puede asumir que la información agregada en un bloque ya no podrá ser modificada (inmutabilidad). La creación de nuevos bloques es realizada por nodos denominados «mineros». Los mineros son nodos de la red que participan en el proceso de escritura de datos en la *blockchain* a cambio de una recompensa económica. La validez de la escritura de un bloque por parte de un minero es revisada y acordada tácitamente por el resto de participantes.

El proceso que permite alcanzar un consenso con garantías entre los mineros de la blockchain para el orden de escritura de bloques es la denominada prueba de trabajo o *Proof-of-work* (PoW). En concreto, para que un bloque sea aceptado, el minero tiene que ser el primero en completar una PoW para el siguiente bloque de la *blockchain*. El PoW es un rompecabezas matemático de dificultad ajustable. En particular, la PoW consiste en encontrar un parámetro (*nonce*) que consiga que al hacer el *hash* sobre todo el bloque (incluido el *nonce*) se obtenga un valor inferior a la dificultad actual establecida por la red. Dicho de otra forma, se trata de encontrar un *nonce* que consiga un valor *hash* del bloque con un determinado número de ceros al inicio. Debido a las características de la función de *hash*, no es posible calcular estos valores analíticamente, es decir, para obtener un bloque válido, el minero debe recurrir a la fuerza bruta: probar valores del parámetro *nonce* hasta hallar uno válido. El proceso de probar valores o fuerza bruta es un proceso computacionalmente costoso, de ahí que este mecanismo se conozca como «prueba de trabajo».

La PoW hace que la creación de bloques con la intención de subvertir el consenso tenga un coste alto para el atacante. Por otra parte, la dificultad de este rompecabezas criptográfico es fácilmente ajustable: se puede incrementar la dificultad aumentando el número de ceros necesarios para completar la PoW o decrementarla reduciendo dicho número de ceros. En particular, en *bitcoin* la dificultad se reajusta cada 2016 bloques (que equivalen a catorce días), con tal de que la creación de nuevos bloques tenga una frecuencia aproximada de un bloque cada diez minutos. La fórmula para dicho ajuste es la siguiente:

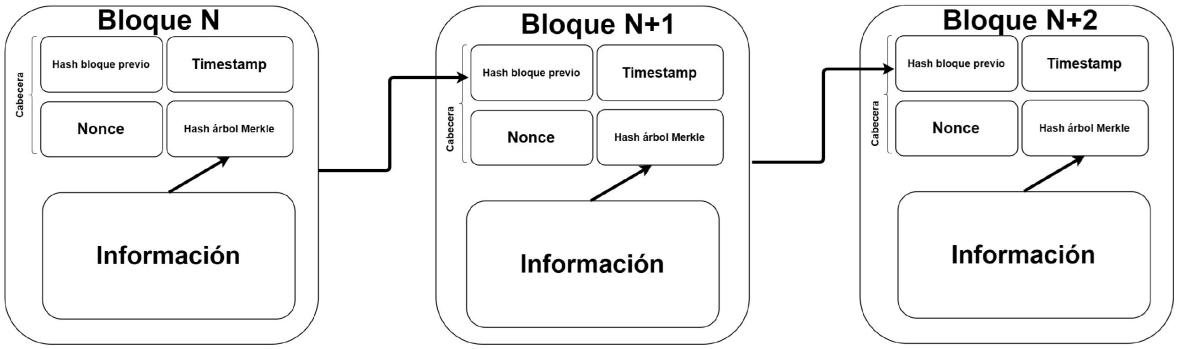
dificultad_nueva = dificultad_previa * 2 semanas / (tiempo en minar los últimos 2016 bloques)

Estructura de los bloques

La *blockchain* almacena una gran cantidad de datos y además su tamaño es creciente con el tiempo ya que en la misma sólo se añade información. Por tanto, es aconsejable disponer de algún mecanismo que permita una consulta a la *blockchain* eficiente, es decir, que permita realizar consultas sin tener que descargar toda la información almacenada. Para este propósito, en la *blockchain* de *bitcoin*, se propone utilizar un árbol *hash* de Merkle (Merkle, 1987, August).

Como se muestra en la Figura 1, el árbol de *hash* de Merkle permite almacenar diversas piezas de información independiente (en el caso de *bitcoin* son transacciones económicas) en las hojas de una estructura en árbol. Para formar el árbol, se hace un *hash* de la información contenida en cada nodo hoja. A continuación, para generar los nodos de

FIGURA 2
ESTRUCTURA DE LOS BLOQUES DE LA *BLOCKCHAIN* DE *BITCOIN*



Fuente: Elaboración propia

cada nivel superior del árbol se concatenan diversos valores *hash* del nivel inferior (dos valores si el árbol es binario) y se le aplica la función *hash* a esta concatenación (ver Figura 1). Repitiendo este proceso se llega a un nivel donde hay un sólo nodo, denominado la «raíz» del árbol.

La ventaja de esta estructura en árbol es que podremos consultar la presencia en dicho árbol de los datos de un cierto nodo/hoja de forma autenticada y sin tener que disponer de toda la información que almacena el árbol. En particular, se puede consultar de forma autenticada cualquier contenido del árbol con una cantidad de valores *hash* proporcional al logaritmo del número de nodos del árbol.

Esto es porque para validar un contenido únicamente hay que proporcionar los nodos adyacentes en cada nivel y el nodo raíz (que tiene contribución de todos los datos almacenados en las hojas) autenticado. Entonces, para validar un contenido se calcula el valor raíz a partir de los nodos adyacentes proporcionados y se comprueba que coincide con el valor raíz autenticado. La estructura es segura porque no se puede generar un conjunto de nodos adyacentes a voluntad que dé como resultado el valor del nodo raíz autenticado. En Muñoz (2004), se puede encontrar una descripción detallada y una implementación eficiente de este tipo de árboles. Por otra parte, en la Figura 2, se muestra la información que contiene cada bloque en la *blockchain* de *bitcoin*:

- El valor *hash* del bloque previo. Este valor permite que los bloques queden vinculados secuencialmente formando una cadena.
- Marca de tiempo (*timestamp*). Esta marca de tiempo permite identificar el instante en el que fue creado el bloque.
- El valor del *nonce*. Este es el valor encontrado por fuerza bruta en el proceso de minado.
- El valor de la raíz del árbol de Merkle de las transacciones (*root hash*). Este valor *hash* permite referenciar toda la información del bloque. Como se ha comentado, con el valor de la raíz del árbol y ciertos valores adiciones se pueden realizar consultas a cerca de la información contenida en un bloque de forma eficiente y segura.
- Información. Por último, el bloque contiene la información en sí.

En el caso de *bitcoin*, la información contenida en los bloques son las transacciones realizadas con la cripto-moneda. En particular, una de las transacciones que debe ser añadida es la que adjudica al creador del bloque una recompensa por haberlo minado. La recompensa por la creación de un bloque se divide entre dos cada 210.000 bloques que equivalen a cuatro años. A su inicio en 2009, la recompensa estaba fijada en 50 *bitcoins* y actualmente, tras el paso de 8 años, esta es de 12,5 *bitcoins*.

Propiedades fundamentales de la blockchain

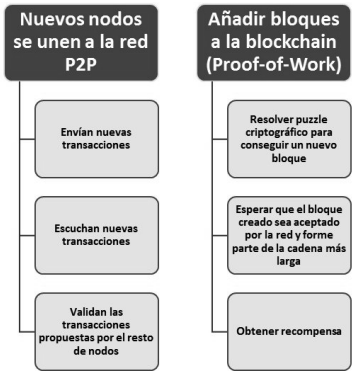
La creación de una *blockchain* robusta debe garantizar dos propiedades fundamentales (Garay, 2015, April):

– Disponibilidad: Asegura que una transacción honesta que ha sido emitida acabe siendo añadida a la cadena de bloques, evitando que se produzca una denegación de servicio (*Denial of Service, DoS*) por parte de nodos corruptos.

– Persistencia: Cuando un nodo da una transacción como estable, el resto de nodos, si son honestos, validarán ésta como estable haciéndola inmutable.

Para cumplir con la propiedad de disponibilidad, la *blockchain* de *bitcoin* (y también la de muchos otros sistemas) implementa una red de nodos interconectados donde dichos nodos interaccionan como iguales (red *peer-to-peer*). La red *peer-to-peer* de *bitcoin* es descentralizada, es decir, cualquier usuario que desee puede contribuir. Otras *blockchain* utilizan un sistema con lista blanca (*white-list*) (Christidis, 2016)

FIGURA 3
ESQUEMA DEL PROCESO SEGUIDO EN *BITCOIN* PARA AÑADIR BLOQUES A LA *BLOCKCHAIN*



Fuente: Elaboración propia

en la que sólo pueden participar los nodos listados. En cualquier caso, los nodos que forman parte de la red *peer-to-peer* disponen, cada uno de ellos, de una copia de la cadena de bloques. La gran cantidad de copias de la *blockchain* proporciona una gran disponibilidad y robustez. En particular, en la inserción de bloques en la *blockchain* mediante la red *peer-to-peer* se distinguen diferentes estados para la información de bloque que está siendo procesada:

- Información candidata a ser añadida: es información que los nodos han enviado al resto de nodos mediante la red *peer-to-peer* pero que aún no ha sido validada en ningún bloque.
- Información confirmada: es información validada por la red y se procede a añadirla al próximo bloque.
- Información estable: es información que forma parte de la *blockchain* de forma inmutable.

En la práctica, se considera que se cumple la propiedad de persistencia para un cierto bloque cuando existen seis bloques minados con posterioridad al mismo (aproximadamente 1 hora de espera). Mediante esta sencilla regla se asegura que una transacción será inmutable con un riesgo inferior al 0,1%, suponiendo que algún atacante tenga más del 10% de la capacidad total de *hash* de la red.

Generación de bloques en la blockchain

La generación de bloques en la *blockchain* se realiza de forma descentralizada. La clave para esta descentralización es que se llegue a un acuerdo sobre qué información se guarda en ella. Para ello, es necesario conseguir un consenso distribuido que permita que los nodos honestos tengan la capacidad de generar la información válida conjuntamente y así evitar que nodos maliciosos puedan guardar información no deseada. En el caso del *bitcoin,* este proceso permite resolver el problema del doble gasto (un usuario gastando dos veces el mismo dinero) que hasta entonces parecía un escollo insalvable para llevar a cabo el uso de monedas digitales.

En la Figura 3 se muestra el proceso seguido en *bitcoin* para añadir bloques a la *blockchain*. En primer lugar, un usuario debe convertirse en nodo dentro del sistema para poder escuchar y emitir nuevas transacciones (información). En segundo lugar, si el usuario desea convertirse en minero y crear nuevos bloques debe competir contra el resto de mineros en la red para resolver el rompecabezas criptográfico y así ser el que escriba el nuevo bloque en la *blockchain* oficial.

El proceso de autenticación de las transacciones se basa en criptografía asimétrica. Cada cuenta de usuario de Bitcoin posee dos llaves relacionadas matemáticamente: una pública (identificador del usuario en la red, conocida por todos) y una privada (secreta, conocida por el usuario). La llave privada se usa para firmar las transacciones emitidas por el usuario; éste especifica las cantidades de moneda a transferir y las llaves públicas de destino. La red y el resto de usuarios, usando la llave pública del emisor, pueden obtener una prueba matemática de que la transacción fue efectivamente firmada por ese usuario y por nadie más, puesto que nadie más tiene su llave privada.

Las nuevas transacciones emitidas son validadas por los nodos más cercanos al emisor, descartando todas las transacciones inválidas y propagando al resto de nodos las transacciones válidas, es decir, aquellas que cumplen con las especificaciones de la red. Posteriormente, se procede a añadir las nuevas transacciones a la cadena de bloques. Este proceso de confirmación de datos se lleva a cabo en *bitcoin* mediante el proceso de minado PoW (aunque en la actualidad están surgiendo otros mecanismos alternativos a PoW como se discute en la siguiente sección).

Finalmente, los nodos comprueban que, en el nuevo bloque creado/minado, todas las transacciones son válidas y que el bloque está correctamente vinculado con su predecesor, es decir, que contiene el *hash* del bloque anterior en su cabecera. En caso afirmativo el bloque es añadido a la *blockchain* incrementando así la cadena. El proceso se repite generando una nueva ronda de minado con las nuevas transacciones emitidas que aún no hayan sido agregadas en ningún bloque anterior de la *blockchain*. Si el bloque es inválido, es descartado, y el resto de nodos siguen el proceso de minado hasta encontrar un bloque válido.

Alternativas a PoW

Existen alternativas a la creación de bloques mediante el minado por PoW. El más usado es el *Proof-of-Stake* (PoS). Su principal diferencia respecto a la PoW es que la creación de bloques es llevada a cabo por nodos que ya poseen la cripto-moneda

CUADRO 1
PRINCIPALES CRIPTO-MONEDAS Y SUS CARACTERÍSTICAS

Cripto-moneda	Fecha Lanzamiento	Market cap [M$]	Algoritmo de Hash	Consenso	Precio [$]
Bitcoin [BTC]	Enero 2009	16050	SHA-256	PoW	992.6
Ethereum [ETH]	Agosto 2015	999	SHA3-256	PoW (PoS)	11.25
Ripple [XRP]	Septiembre 2013	233	ECDSA	Byzantine Consensus	0.006295
LiteCoin [LTC]	Octubre 2011	185	Scrypt	PoW	3.73
Monero [XMR]	Mayo 2014	170	Cryptonight	PoW	12.22
Dash [DASH]	Enero 2014	120	X11	PoW/PoS	16.93

Fuente: Elaboración propia

subyacente (*stakeholders*), lo que por sí solo consigue que no haya interés en corromper el correcto funcionamiento del sistema. Este protocolo asigna una probabilidad de crear bloques proporcional a la cantidad de moneda que posee cada nodo. Así, aquellos usuarios que tengan más cantidad de la cripto-moneda serán los que creen bloques con más frecuencia.

La principal ventaja respecto al PoW es que la creación de bloques no requiere potencia de computación para su correcto funcionamiento lo que, por sí mismo, es una gran ventaja. En la actualidad el minado de *bitcoins* genera un gran gasto de energía con el único objetivo de mantener robusto el sistema. Como referencia cabe destacar que en el año 2014 la PoW de *bitcoin* ya consumía tanta energía eléctrica como lo hacía toda Irlanda (O'Dwyer, 2014).

La principal desventaja es que el sistema podría llegar a no ser descentralizado. Para evitar que esto pase han surgido diferentes métodos que solventan el problema. En ellos se pondera el *stake* de cada propietario junto con la duración que hace que este lo posea con tal de asignar una probabilidad para la creación del próximo bloque. Varios ejemplos de implementaciones con PoS son Kiayias (2016), Bentov (2014) y Mizrahi (2014).

En el esquema (Cuadro 1) se pueden observar las principales cripto-monedas existentes (con más valor de mercado) con el método de consenso usado. Además, se incluye información relevante como el algoritmo de *hash* que usan, su precio y su capitalización (Farell, 2015).

APLICACIONES

A día de hoy *bitcoin* es, sin duda alguna, la realización práctica de la tecnología *blockchain* más conocida. Sin embargo, la lista de posibles casos de uso es mucho más larga y potencialmente más revolucionaria que la cripto-moneda, que se está erigiendo como sistema alternativo de pagos a nivel mundial. A continuación, se describen algunas de dichas aplicaciones y casos de uso.

Cripto-monedas

Una *blockchain* puede diseñarse como una base de datos verdaderamente descentralizada y sin una autoridad central. Puede, por tanto, servir como centro de intercambios de confianza entre múltiples entidades sin que unas deban confiar en la otras, ni tan siquiera en un intermediario. Esto representa una verdadera revolución: en los sistemas de intercambio ha existido históricamente la necesidad de un intermediario de confianza de todas las partes. Por ejemplo, cuando alguien compra un objeto de segunda mano en una plataforma online, ésta se encarga de verificar, a cambio de un porcentaje, que la transacción se ha realizado con éxito y de compensar a las partes en caso de fraude. O, análogamente, cuando un banco acuerda un préstamo con una empresa, el acuerdo se explicita en un contrato con validez legal: el Estado, con sus poderes coercitivos, es el garante del cumplimiento del contrato. Nada de esto es necesario en la *blockchain*.

En el caso de las monedas clásicas, existe además una autoridad monetaria: los bancos centrales. Éstos son los únicos con la capacidad de emitir más unidades monetarias: se encuentran en la base de la cadena crediticia y tienen cierta potestad para determinar el precio base del crédito. Estas decisiones se toman habitualmente respondiendo a criterios de política macroeconómica tales como: estabilidad a largo plazo, objetivos de inflación, relación importaciones/exportaciones, etc.

Las cripto-monedas basadas en *blockchains* eliminan también la necesidad de una autoridad central. El criterio de emisión de nuevas unidades monetarias se encuentra prefijado. En el caso del *Bitcoin*, por ejemplo, se emite nueva moneda cada vez que se mina un bloque (cada 10 minutos aproximadamente) y se pone en posesión del nodo que lo ha minado. La cantidad decrece aproximadamente cada cuatro años y el sistema está diseñado para llegar a un total de 21 millones de *bitcoins* en 2040. Desaparece, por tanto, la incertidumbre asociada a este tipo de decisiones políticas. Se elimina, además, la posibilidad de que los Estados usen los

bancos centrales para beneficiar a unos sectores o perjudicar a otros.

Existen decenas de cripto-monedas. Todas ellas comparten su utilidad como sistema de pago. Algunas utilizan una *blockchain* propia y otras funcionan encima de la *blockchain* de *bitcoin*. Su funcionamiento es bastante heterogéneo y todas ellas pretenden aportar alguna mejora respecto a *bitcoin*.

Probablemente, la más prometedora entre las alternativas es *Ethereum*, que es la segunda cripto-moneda con mayor capitalización (Cuadro 1). *Ethereum* cuenta con una *blockchain* propia, es decir, distinta a *bitcoin* y por el momento también basada en PoW (aunque tiene planeada una migración a PoS). Más allá de su funcionamiento como cripto-moneda, la aportación principal de *Ethereum* son los contratos inteligentes (*Smart Contracts*) (Buterin, 2014). Los contratos inteligentes son *scripts* (pequeños códigos) auto-ejecutables que residen en la *blockchain* y que permiten automatizar gran cantidad de procesos comerciales de una forma segura y transparente para todos los participantes. Los ejemplos del siguiente apartado representan algunos usos potenciales de este tipo de funcionalidad.

Blockchain e IoT

Sistema de distribución de *firmware* (Christidis, 2016)**.** A medida que la Internet de las cosas (*Internet of Things, IoT*) vaya convirtiéndose en realidad, el número de dispositivos conectados a la red de redes crecerá exponencialmente (The internet of everything, 2015). Ahora, además de computadores y equipos red, se van conectando a Internet electrodomésticos, dispositivos de vigilancia y seguridad, sensores de todo tipo, etc. Sin duda este nuevo ecosistema ofrece una flexibilidad sin precedentes. Sin embargo, este paradigma tiene también algunos retos a resolver. Entre ellos, destaca sobremanera el ámbito de la seguridad. Por ejemplo, varias fuentes afirman que el reciente ataque a los servidores de DNS del proveedor DynDNS, que dejaron sin servicio durante horas a gigantes como Twitter o Facebook, se realizaron controlando remotamente un gran número de dispositivos de IoT (Hackers Used New Weapons to Disrupt Major Websites Across U.S., 2016).

Uno de los primeros problemas de seguridad que aparece en el entorno IoT es el nivel de supervisión de los dispositivos. En este sentido, en el entorno IoT, muchos dispositivos no están supervisados con los niveles usados en el mundo de la computación (ordenadores personales o teléfonos inteligentes). Además, por su bajo coste, muchos de estos dispositivos no siempre reciben actualizaciones con una elevada frecuencia por parte de los fabricantes (o incluso se quedan sin actualizar en algún punto). Para los fabricantes resulta bastante costoso tener que enviar directamente a millones de dispositivos actualizaciones y realizarlo incluso después de años de haber abandonado la fabricación de tales dispositivos.

Al mismo tiempo, para el consumidor, existe cierta desconfianza en dispositivos que se comunican con su fabricante sin la supervisión del usuario final y sería mucho mejor un enfoque de seguridad más transparente. Este escenario, bien podría solucionarse con una *blockchain*. En este caso, se aprovecharía tanto su característica de sistema distribuido y su transparencia, como su robustez y fiabilidad. Los dispositivos consultarían la *blockchain* para averiguar si su *firmware* está actualizado. En caso que no lo esté, pedirían a otros nodos que les manden la nueva versión. Una vez recibida, podrían usar el código de la *blockchain* para comprobar que el *firmware* no ha sido alterado en modo alguno, evitando así las intrusiones. Este enfoque, una vez implementado, resultaría bastante más barato para el fabricante que sólo tendría que mandar la actualización a unos pocos nodos y dejar que la actualización propague.

Mercado de servicios entre dispositivos. Si a una cripto-moneda se le añade capacidad para contratos inteligentes, la aplicabilidad en IoT se dispara. En el caso anterior, por ejemplo, los dispositivos que mandan el nuevo *firmware* podría tener una pequeña remuneración, ya que consumen recursos (electricidad y ancho de banda). La idea es, en general, que cada aparato conectado a la *blockchain* tenga su propia «cuenta bancaria» y ofrece sus servicios en el ecosistema. *Filecoin* (FileCoin: A Criptocurrency Operated File Storage Network, 2017), por ejemplo, permite a sus nodos alquilar espacio de almacenamiento. Por otra parte, *EtherAPIs* (EtherAPIs: Decentralized, anonymous, trustless APIs, 2017) sirve para monetizar llamadas remotas a un programa determinado.

En el mercado de la energía, esta arquitectura resulta especialmente útil. La entrada de las renovables como factor de peso y la proliferación de sistemas de almacenamiento (bancos de baterías y baterías en casa) ha vuelto el ecosistema más heterogéneo de lo que ya era. Hay productores que producen de forma constante (p.ej. central nuclear), otros sólo durante el día (placas solares) y otros sólo cuando hace viento (generadores eólicos). La demanda tiene horas muy intensivas y otras de muy bajo consumo.

Una batería conectada a la red, por ejemplo, podría comprar energía en las horas de bajo precio para luego venderla en las horas puntas, según las normas definidas por el propietario. *TransActive Grid* (Transactive Grid: Secure, transactional control of utility systems, 2017), por ejemplo, está experimentando con este concepto de mercado entre aparatos. Aunque muchas de estas funcionalidades ya se realizan actualmente, la tecnología *blockchain* permitiría hacerlo en un ecosistema unificado, seguro, versátil, transparente y barato.

Sistema de seguimiento de transportes. En un envío internacional de mercancías participan normalmente varias empresas ya que se utilizan varios medios de transporte. Todas ellas tienen sus bases de datos independientes donde actualizan el estado del envío

en función de la información proporcionada por las otras o por sus agentes. *Blockchain* tiene aquí una clara aplicabilidad que permitiría hacer el sistema más simple, más transparente y menos costoso. Para empezar, la base de datos (la propia *blockchain*) sería compartida por todos los intermediarios y por el remitente y destinatario, reduciendo los costes. No sería para ello necesaria la confianza entre ellos en general. Al llegar el contenedor en cuestión a un cierto puerto, se añadiría una actualización a la base de datos. Al estar todas las actualizaciones firmadas con las claves privadas del que entrega y el que recoge y con la clave del contenedor, esta actualización actuaría como prueba criptográfica de que el contenedor se encuentra ahora en posesión del administrador del puerto. Además, el sistema incluye marcas de tiempo (*timestamps*) para hacer el seguimiento. La transparencia y fiabilidad del concepto ayudaría sin duda a la resolución de disputas entre los participantes.

Si a este enfoque innovador se le añade IoT se puede ganar aún más eficiencia. Los contenedores y los lugares de intercambio pueden tener dispositivos incorporados que automaticen totalmente el proceso, disminuyendo los costes aún más y reduciendo las probabilidades de error y de fraude.

Prueba de existencia

Una de las características más notables de *blockchain*, sino la más notable, es su inmutabilidad: una vez una información se ha añadido a la base de datos distribuida, y añadidos unos pocos bloques detrás, la probabilidad de que sea modificada es, a efectos prácticos, cero.

Esta propiedad, sin equivalente en el mundo digital ni en el mundo real, tiene obvias aplicaciones. Tradicionalmente, si alguien quiere probar públicamente ser el autor de una información, sea un diseño tecnológico o una canción, acude a una oficina de patentes o similar. Esto es, como pasaba con las transacciones, una entidad de confianza de todas las partes que ofrece, básicamente, la garantía de no modificar nada y de no revelar nada (a excepción de lo necesario para una potencial batalla legal, siempre autorizado por el propietario). La tecnología *blockchain* puede sustituir también a este intermediario.

Por ejemplo, en *Proof of existence* (2017) se ha implementado un servicio donde cualquiera puede generar una prueba de que una información existía en un momento determinado en el tiempo y almacenarla en la *blockchain* de *Bitcoin*. El funcionamiento es sencillo: se calcula un *hash* para el documento en cuestión. Del *hash* no se puede deducir el documento, pero sólo el poseedor del documento puede haber generado el *hash*. Luego se genera una transacción especial que permite almacenar este código en la *blockchain*. La transacción se envía y una vez es añadida en un bloque, queda ahí para siempre. El bloque contiene, además, fecha y hora, tan inmutables como el resto, completando así la prueba segura, pública y verificable de existencia. Además, su coste es ínfimo, sobre todo comparado con los costes de las patentes convencionales.

En cuanto al propietario del documento, sus datos pueden encontrarse en el mismo documento. Debido a las propiedades de la función de *hash*, cualquier cambio, por pequeño que sea, resulta en un *hash* totalmente diferente. El sistema tiene ahí otra utilidad derivada: comprobación de integridad de documentos. Un usuario puede comprobar mediante la misma página web que un cierto documento original almacenado en la *blockchain* es idéntico al que posee.

Seguridad en *Big Data* mediante *blockchain*

Varias técnicas de *big data* se usan actualmente para analizar la *blockchain* e incrementar sus niveles de seguridad. Estas técnicas permiten deducir las identidades de los nodos en las cripto-monedas, detectar fraudes y mapear los flujos reales de dinero (Reid, 2013), (Farell, 2015).

La relación inversa, sin embargo, es aún más prometedora: utilizar la tecnología *blockchain* para dar seguridad y verificabilidad a entornos empresariales de *big data*. Con la explosión del *big data*, prácticamente toda empresa con un mínimo de clientes está interesada en sacar el máximo partido a sus datos para así mantenerse competitiva. Se trata de datos que habitualmente provienen de diversas fuentes, en diversos formatos, y son utilizados en diversos procesos por distintos departamentos de la empresa. Los peligros de estos sistemas resultan bastante evidentes: manipulación de los datos por parte de trabajadores internos, proveedores maliciosos, corrupción de los datos, fallos de almacenamiento, uso defectuoso, incumplimiento de legislaciones respecto a los datos personales y un largo etcétera.

En este contexto, la *blockchain* tiene mucho que aportar: transparencia, verificabilidad, portabilidad y escalabilidad. Mediante *blockchain*, cada añadido en los datos, cada cambio, cada extracción para su uso o cada visualización se podría realizar utilizando un registro transparente y seguro. Además, los datos podrían ir acompañados de pruebas de integridad a bajo nivel o incluso, en el caso de la extracción, de firmas concretas que posibiliten su trazabilidad.

Estos entornos permiten un grado de seguridad y verificabilidad suficiente para cumplir con regulaciones bastante restrictivas a la vez que son intrínsecamente distribuidos, escalables e interoperables. Los requisitos legales en cuanto a la retención de datos dejan de ser un problema pues está en la propia naturaleza de *blockchain* el poder deducir

el estado de la base de datos en cualquier punto del tiempo.

La herramienta *Hadoop Big Data Lakes* de la empresa *Guardtime* es un ejemplo de este tipo de tecnología (GuardTime: Hadoop Big Data Lakes, 2017).

CONCLUSIÓN

La *blockchain* permite implementar una base de datos distribuida, pública e inmutable basada en una secuencia creciente de bloques. Esta base de datos proporciona de forma intrínseca tolerancia a fallos en nodos, robustez frente a manipulación y al ser pública, transparencia. Los usos de esta tecnología son potencialmente inmensos y por ello se considera como una de las tecnologías con más potencial disruptivo de los últimos años.

La posibilidad de tener una base de datos distribuida e inmutable a posteriori tiene un sinfín de utilidades prácticas que solo empiezan a vislumbrarse. Las cripto-monedas han sido su primera aplicación de éxito debido a las necesidades de seguridad y transparencia de los sistemas de pago y a la posibilidad de eliminar intermediarios. En el futuro, sin embargo, es posible que encontremos sistemas de blockchain en una infinidad de contextos y sistemas. En este sentido, y como punto de partida, se pueden considerar los casos de uso en escenarios como Internet de las cosas (IoT) y big data mencionados en este artículo.

BIBLIOGRAFÍA

BENET, J. (2014). IPFS-content addressed versioned, P2P file system. arXiv preprint arXiv:1407.3561.

BENTOV, I. L. (2014). «Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake» [Extended Abstract]. *ACM SIGMETRICS Performance Evaluation Review*, 42(3), 34-37.

BITCOIN PRICE INDEX. (13 de Feb de 2017). Obtenido de CoinDesk: http://www.coindesk.com/price/Blockchain holds key to reinventing energy grid. (s.f.). Obtenido de http://www.huffingtonpost.com/don-tapscott/blockchain-holds-key-to-r_b_11258136.html

BUTERIN, V. (2014). «A next-generation smart contract and decentralized application platform». *white paper*.

CHRISTIDIS, K. &. (2016). «Blockchains and Smart Contracts for the Internet of Things». *IEEE Access*, 4, 2292-2303. EtherAPIs: Decentralized, anonymous, trustless APIs. (2017). Obtenido de EtherAPIs: etherapis.io

FARELL, R. (2015). «An analysis of the cryptocurrency industry.»

FILECOIN: A Criptocurrency Operated File Storage Network. (2017). Obtenido de FileCoin: filecoin.io

GARAY, J. K. (2015, April). «The bitcoin backbone protocol: Analysis and applications». *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 281-310). Springer Berlin Heidelberg.

GUARDTIME: Hadoop Big Data Lakes. (2017). Obtenido de GuardTime: https://guardtime.com/solutions/hadoop-big-data-lakes Hackers Used New Weapons to Disrupt Major Websites Across U.S. (Oct de 2016). Obtenido de NYTimes: https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0

KIAYIAS, A. R. (2016). «Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol».

MERKLE, R. C. (1987, August). «A digital signature based on a conventional encryption function». *Conference on the Theory and Application of Cryptographic Techniques* (pp. 369-378). Springer Berlin Heidelberg.

MIZRAHi, I. B. (2014).» Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake».

MUÑOZ, J. L. (2004). «Certificate revocation system implementation based on the Merkle hash tree». *International Journal of Information Security*, 2(2), 110-124.

NAKAMOTO, S. (2008). «Bitcoin: A peer-to-peer electronic cash system».

O'DWYER, K. J. (2014). «Bitcoin mining and its energy footprint». Proof of existence. (2017). Obtenido de Proof of existence: https://proofofexistence.com/

REID, F. &. (2013). «An analysis of anonymity in the bitcoin system». *Security and privacy in social networks* (pp. 197-223). Springer New York.

RON, D. &. (2013, April). «Quantitative analysis of the full bitcoin transaction graph». *International Conference on Financial Cryptography and Data Security* (pp. 6-24). Springer Berlin Heidelberg. The internet of everything. (2015). Obtenido de Business Insider: http://www.businessinsider.com/internet-of-everything-2015-bi-2014-12

TRANSACTIVE GRID: Secure, transactional control of utility systems. (2017). Obtenido de Transactive Grid: http://transactivegrid.net/