ue STEAM essentials

BLOCKCHAIN

SUSANA DEL POZO
Ingeniero de Telecomunicaciones
UNIVERSIDAD DE VALLADOLID

Blockchain, cadena de bloques en inglés, es un registro digital que está repartido entre varios participantes sin que exista una autoridad central. Puede decirse que es una base de datos de transacciones descentralizada y distribuida entre varios nodos. Se caracteriza por el hecho de que para hacer actualizaciones es necesario el consenso de la mayoría de los participantes y la información introducida nunca puede ser borrada. Surgida de una criptomoneda, blockchain ha pasado a ser considerada una tecnología disruptiva para el mundo empresarial.

PALABRAS CLAVE •
Blockchain, Bitcoin, Ethereum, NFT

CÓMO CITAR ESTE ARTÍCULO •
del Pozo, Susana. 2021. **"Blockchain"** en: UEM STEAM Essentials

INTRODUCCIÓN

Blockchain es una tecnología que permite realizar transacciones punto a punto entre participantes. Estos participantes o nodos se conectan entre sí constituyendo una red en la que no hay un nodo central. Blockchain permite establecer relaciones de confianza entre los participantes. Puede verse como un registro digital o una base de datos de transacciones que está distribuida entre todos los nodos participantes.

El primer diseño de una aplicación de lo que ahora llamamos blockchain aparece en el artículo de 2008 que da origen a la criptomoneda bitcoin. El artículo muestra una forma novedosa de combinar tecnologías que se habían desarrollado en las décadas de los 70 y los 90 fundamentalmente para crear un sistema de pagos online sin recurrir a instituciones financieras.

Las tres características principales de una solución blockchain son descentralización, inmutabilidad y transparencia. Blockchain se basa en una **tecnología descentralizada** que permite la desintermediación: las funciones que en un sistema tradicional realizarían intermediarios (bancos, instituciones, mercados, etc.) las realizan de forma distribuida y sin una autoridad central todos los participantes de la red. Blockchain garantiza la **inmutabilidad**. Gracias a la utilización de algoritmos criptográficos, el libro de registro que se soporta sobre la infraestructura de blockchain no puede ser modificado. También aporta **transparencia**, ya que todos los nodos tienen acceso tanto a la información del estado actual como al registro de trazabilidad de las acciones que han desembocado en ese estado.

En este documento vamos a explicar el funcionamiento de las redes blockchain, los tipos de redes existentes, las implementaciones más extendidas, el impacto de blockchain sobre la sostenibilidad y los casos de uso de esta tecnología.

FUNCIONAMIENTO DE UNA RED BLOCKCHAIN

En una red blockchain nos encontramos con transacciones efectuadas entre nodos. Blockchain nos va a permitir crear un registro descentralizado e inmutable de dichas transacciones utilizando bloques que las agrupan. El mecanismo de funcionamiento básico es el siguiente:

1 » Los usuarios crean transacciones. Los usuarios cuentan con una clave pública y una privada. La clave pública puede asemejarse a un número de cuenta y la privada a una firma. A modo de ejemplo, si un usuario quiere hacer una transacción que consiste en el envío de dinero a otro, este último tiene que facilitarle su clave pública y el primero utilizará su propia clave privada para firmar la transacción. Esto se conoce como criptografía asimétrica.

2 » Una vez creada una transacción el usuario solicita su ejecución a través de un nodo participante en la red.

3 » La transacción es validada formal y sintácticamente y difundida por otros nodos de la red, de manera que la información se propaga rápidamente y cada nodo dispone siempre de la información actualizada.

4 » Las transacciones se agrupan en bloques y los bloques se van enlazando, formando la cadena. Para decidir cuál es el siguiente bloque que se añadirá a la cadena se utiliza un protocolo de consenso.

5 » Una vez que se ha añadido el bloque a la cadena ya no puede ser borrado ni alterado.

Para asegurar la inmutabilidad que caracteriza a blockchain se utiliza el concepto de hash del bloque. Un hash es un identificador único de una secuencia de datos. Es el resultado de una función hash, una operación criptográfica que genera identificadores únicos de longitud fija a partir de una cantidad de datos de tamaño arbitrario. Cualquier modificación, por pequeña que sea, en los datos de entrada produce una modificación del hash asociado a esos datos.

Los procesos de creación de bloques y consenso se llevan a cabo de la siguiente manera:

1 » Los nodos efectúan una validación formal de las transacciones de manera independiente. Validan aspectos tales como que la sintaxis es correcta, que las cantidades son coherentes o que las direcciones son válidas.

2 » Las transacciones que no superan la validación son rechazas y las válidas son enviadas a un pool de transacciones no confirmadas.

3 » Unos nodos especiales, que generalmente se denominan mineros, cogen transacciones del pool para crear los bloques.

4 » Para decidir qué minero tiene el derecho de añadir el siguiente bloque a la cadena, éstos aplican un protocolo de consenso o algoritmo que difiere según la red blockchain de la que se trate. En el caso de Bitcoin, por ejemplo, el algoritmo consiste en resolver un reto criptográfico que requiere muchos recursos de CPU y que está asociado al hash del bloque que se quiere añadir. Una vez que un minero ha resuelto el reto, se anuncia y el bloque es difundido a la red. El minero recibe en general una compensación por haber producido el bloque y una comisión por las transacciones incluidas en el mismo.

5 » El nuevo bloque es validado por otros participantes y se alcanza un consenso para añadirlo a la cadena. Al añadir los nodos el bloque a su copia local de la cadena, las transacciones incluidas en dicho bloque quedan confirmadas.

A continuación, se describe en detalle la estructura de los bloques, así como el uso de las funciones hash y el procedimiento por el cuál un minero gana el derecho de añadir un bloque a la red.

ESTRUCTURA Y ENLAZADO DE BLOQUES

Los bloques están formados por una cabecera y un cuerpo en el que están los datos de las transacciones válidas incluidas en el bloque.

Las transacciones del bloque se almacenan mediante una estructura denominada árbol de Merkle. Esta estructura de almacenamiento tiene ciertas peculiaridades: para cada transacción se calcula un hash, éstos se agrupan en pares para generar a su vez un nuevo hash y así sucesivamente hasta llegar a un único hash denominado nodo raíz o raíz de Merkle que representa un identificador único de todo el grupo de transacciones, tal y como aparece reflejado en la Figura 1. La característica diferencial de esta forma de almacenamiento es que permite verificar de forma muy rápida una gran cantidad de registros de datos.

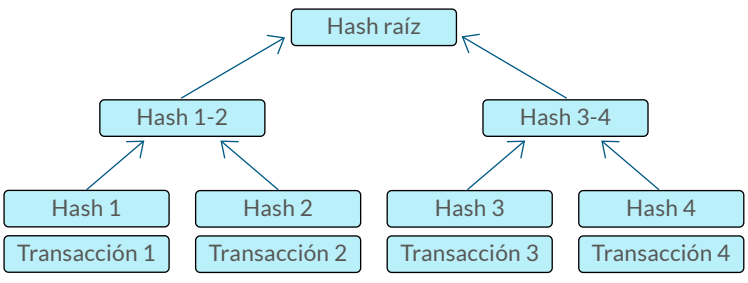

Figura 01 » Árbol de Merkle **(Fuente: propia, 2021)**

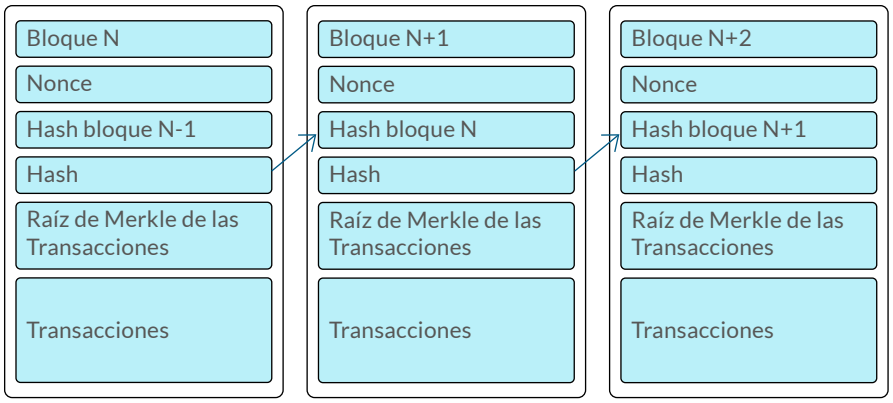

Figura 02 » Estructura de la cadena de bloques **(Fuente: propia, 2021)**

En la cabecera del bloque se incluyen:

» El identificador del bloque

» La raíz de Merkle del árbol que contiene las transacciones

» El hash del bloque anterior

» El hash del bloque actual

» El nonce, o "number that can be only used once" (número que solo puede usarse una vez).

El nonce es un número arbitrario fundamental para garantizar la inmutabilidad de la cadena de bloques como veremos más adelante.

El hash del bloque actual se calcula aplicando una función hash a toda la cabecera del bloque, así que recoge toda la información de las transacciones y los bloques anteriores.

Tal y como se muestra en la Figura 2, el hecho de que cada bloque incluya en su cabecera el hash del bloque anterior crea una cadena enlazada de bloques y hace que el hash de cualquier bloque de la cadena dependa de todos los bloques generados con anterioridad. Esta idea de crear dependencia entre los bloques de una cadena apareció por primera vez en la patente de IBM 4074066 del año 1976.

CLASIFICACIÓN DE REDES BLOCKCHAIN

Las redes blockchain se pueden clasificar en tres grupos según el tipo de relación de confianza entre los nodos participantes tal y como aparece en la Tabla 1.

PROTOCOLO DE CONSENSO

El protocolo de consenso es un elemento clave de las redes blockchain porque permite añadir el siguiente bloque a la cadena de forma segura.

En blockchains privados, en los que existe una relación de confianza entre los nodos, se utilizan protocolos de consenso basados en votación que fundamentalmente buscan conseguir agilidad y tolerancia a errores. Sin embargo, en

TIPO	ACCESO	TRANSPARENCIA	EJEMPLOS
Públicas	Cualquiera puede unirse	Las transacciones pueden ser vistas por cualquiera	Bitcoin Ethereum
Privadas	Por invitación	Las transacciones son privadas	Hyperledger Fabric, creada por la Fundación Linux Corda, diseñada para el sector financiero
Híbridas o Federadas	Por invitación	Pueden existir transacciones privadas y públicas	we.trade, una plataforma para operaciones de comercio internacional que integra a 16 bancos

Tabla 01 » Tipos de redes blockchain **(Fuente: propia, 2021)**

blockchains públicos, donde los participantes no se conocen y es posible la presencia de nodos maliciosos, los protocolos de consenso son los que deben aportar confianza.

El mecanismo más extendido en blockchains públicos se denomina Proof of Work (PoW). En PoW, para poder añadir el siguiente bloque a la cadena, se exige que su hash tenga ciertas características lo que constituye un desafío criptográfico: por ejemplo, que el hash del bloque sea menor que un cierto número, es decir, que empiece por un número concreto de 0s. Este desafío solo puede resolverse por azar, repitiendo el cálculo del hash mientras se varía el valor de un elemento de la cabecera denominado nonce. El nodo que encuentra el nonce adecuado completa el bloque y lo difunde a los demás nodos. Se trata de un problema difícil de resolver computacionalmente pero fácil de comprobar.

Una vez creada la cadena, si un actor malicioso quisiera modificar una transacción, no sólo tendría que hallar el nonce adecuado para recalcular el hash del bloque que contiene la transacción, sino que debería hallar los nonce de todos los bloques posteriores y recalcular sus hashes para que la cadena siguiera siendo válida. Se puede demostrar que, si la mayoría de la capacidad de cómputo de la red está en manos de nodos honestos, la probabilidad de que un actor malicioso tenga éxito recalculando la cadena manipulada antes de que otro nodo añada un bloque lícito, y por tanto invalide su intento de cometer fraude, tiende a cero. Si bien es una manera de proporcionar confianza en redes blockchain públicas, tiene la desventaja de una gran ineficiencia de recursos y una pobre escalabilidad.

EJEMPLOS DE REDES BLOCKCHAIN

» Bitcoin

Bitcoin fue la primera red y aplicación de blockchain. Se trata de una moneda digital puesta en circulación en 2009 por una persona o grupo anónimo conocido por el pseudónimo de Satoshi Nakamoto.

Aunque la utilidad fundamental de la red Bitcoin es realizar transacciones en las que se intercambia dinero representado por bitcoins, no existe el concepto de una cuenta ni el registro del saldo de cada usuario. El funcionamiento de Bitcoin es más similar al de una billetera. El usuario tiene una serie de "monedas", que pueden tener cualquier valor arbitrario. Estas "monedas" han sido recibidas como resultado de transacciones anteriores y no se han gastado. Esto se denomina Unspent Transaction Output (UTXO). Cuando el usuario quiera realizar una nueva transacción, cogerá una o varias monedas cuyo valor sea igual o superior al de la transacción que quiere realizar y las gastará, entregando la cantidad que desee al destinatario y generando el cambio correspondiente con el que se quedará.

A modo de ejemplo, si una persona llamada Alice tiene 5 bitcoins como resultado de una transacción y 15 como resultado de otra, y quiere dar 17 a un destinatario llamado Bob, tiene que ejecutar una nueva transacción que tendrá 2 entradas (UTXO) y 2 salidas (UTXO):

Figura 03 » Transacción bitcoin **(Fuente: propia, 2021)**

En Bitcoin las monedas solo se pueden utilizar una vez. En el momento en que se realiza la transacción, las entradas quedan gastadas y las monedas desaparecen, creándose monedas nuevas que se reflejan en las salidas.

Una vez realizada la transacción, ésta se difunde por la red de nodos de Bitcoin y pasa a formar parte del pool de transacciones. Los mineros cogerán la transacción del pool, la validarán y la añadirán a un bloque. Esta tarea consume recursos de computación y energía y los mineros suelen recibir una comisión por esta labor. La comisión, que es definida por el usuario que genera la transacción, es la diferencia entre el valor total de las salidas y el valor total de las entradas. En el ejemplo anterior no había comisión, pero esto no es habitual, ya que los mineros generalmente eligen procesar en primer lugar las transacciones con la que reciben mayor comisión.

» Ethereum

Ethereum fue concebida por el desarrollador Vitalik Buterin que, tras darse cuenta de que blockchain podía tener muchas otras aplicaciones más allá de las criptomonedas, publicó un artículo en 2013 al que se unieron otros desarrolladores y que desembocó en el lanzamiento de Ethereum el 30 de julio de 2015.

En el documento publicado, Vitalik Buterin explica cómo la tecnología de blockchain puede ser útil para el desarrollo de una gran variedad de aplicaciones descentralizadas. Para ello propone añadir a una capa de blockchain base, similar a la de Bitcoin, un lenguaje de programación completo en el

sentido de Turing -lo que implica que soporta estructuras complejas tipo bucles y que puede abordar escenarios de programación generales. Este lenguaje de programación permite desarrollar "smart contracts", que en palabras de Vitalik son cajas criptográficas que contienen elementos de valor y que solo se liberan cuando se cumplen ciertas condiciones. El documento de Vitalik incluye un ejemplo ilustrativo. Se trata de una libreta protegida por una clave donde Alice quiere mantener ahorros. Alice teme perder la clave para acceder a la libreta o que le roben todo su dinero. Para evitar esto, Alice puede establecer un contrato con Bob para que le ayude a mantener seguros sus ahorros, de manera que:

» Alice siempre puede sacar hasta un 1% de los ahorros cada día, limitando así la cantidad que le puede ser robada si alguien se hace pasar por ella.

» Alice y Bob juntos pueden retirar cualquier cantidad, permitiendo a Alice acceder a todo su dinero si lo necesita.

» Bob puede sacar hasta un 1% por el servicio que presta.

» Alice puede retirar la autorización a Bob en cualquier momento si decide prescindir de su servicio.

Estas reglas pueden codificarse de forma sencilla en un programa, el smart contract, que se ejecuta en la red de blockchain garantizando su cumplimiento. En la práctica estas reglas estarían haciendo que Bob jugase un papel similar al que realiza un banco.

Otro elemento diferencial que se refleja en el documento es que Ethereum utiliza el paradigma de las cuentas en lugar del modelo UTXO de Bitcoin. Las cuentas mantienen un saldo que se denomina en Ethers y pueden estar controladas por claves privadas de usuarios (cuentas externas) o por el código de un smart contract (cuentas de contrato). En el ejemplo anterior Alice y Bob tendrían seguramente sus propias cuentas externas y existiría una cuenta de contrato que contiene los ahorros de Alice. Tal y como se ve en el ejemplo, a pesar de su nombre, el smart contract no es un vínculo legal que deba cumplirse, sino que se comporta como un agente autónomo que controla el acceso a una cuenta.

Aunque el ejemplo anterior está relacionado con movimientos de dinero, es importante destacar que otra de las aportaciones de Ethereum fue introducir la capacidad de realizar transacciones no solo de una criptomoneda sino de cualquier tipo de activo representado por un "token". Los tokens pueden representar prácticamente cualquier cosa: inversiones en activos financieros (security tokens), derechos de uso de un producto o servicio (utility tokens), reputación, habilidades, etc. Utilizando smart contracts es posible realizar operaciones tales como compras, ventas o intercambios con estos tokens, beneficiándose de las características de descentralización, inmutabilidad y transparencia de la red de blockchain.

» Hyperledger Fabric

Hyperledger Fabric es un proyecto de la comunidad open source Hyperledger, lanzada por la Fundación Linux a principios de 2016 con el objetivo de apoyar proyectos relacionados con blockchain orientado a entornos empresariales. El proyecto Hyperledger Fabric fue propuesto en marzo de 2016 y tras una etapa de incubación, se activó a principios de marzo de 2017.

Hyperledger Fabric se basa en que todos los participantes de la red son conocidos y existe una relación de confianza entre ellos. Es por tanto una red privada a la que no pueden sumarse nodos de manera espontánea.

En Hyperledger Fabric no existe el concepto de criptomoneda. El modelo intenta representar las relaciones existentes en el mundo de la actividad empresarial y permite definir casi cualquier activo de valor, como por ejemplo propiedades inmobiliarias, equipamiento, propiedad intelectual, relaciones contractuales, etc.

Al igual que los smart contracts de Ethereum controlan cuentas, Hyperledger Fabric permite crear código que define, modifica y controla los activos. Se denomina chaincode y es la lógica de negocio.

Posiblemente la mayor diferencia de Hyperledger Fabric frente a redes públicas como Bitcoin y Ethereum es el algoritmo de consenso que se utiliza para validar las transacciones y construir el siguiente bloque de la cadena. Hyperledger Fabric permite elegir mecanismos diferentes y el más habitual es el protocolo RAFT, que consiste en un mecanismo de votación. Esto es factible puesto que existe una relación de confianza entre los nodos.

BLOCKCHAIN Y SOSTENIBILIDAD

Es creciente la preocupación por el impacto ambiental de las redes de blockchain públicas, debido a que resolver el desafío criptográfico del mecanismo Proof of Work (PoW) requiere un altísimo número de operaciones.

Bitcoin supone un porcentaje relevante de todo el consumo mundial de electricidad. A fecha de mayo de 2021, según la Universidad de Cambridge, Bitcoin tiene un consumo de energía equiparable al de países como Suecia, Argentina, Holanda o Noruega.

El consumo energético de Ethereum también es elevado. Uno de los cambios más relevantes de Ethereum 2.0 y que

se espera para 2021 es la sustitución del mecanismo PoW por un mecanismo de consenso alternativo denominado Proof of Stake (PoS) que no utiliza una potencia de cómputo elevada. En el mecanismo de PoS los mineros no compiten entre ellos para crear el próximo bloque resolviendo un acertijo criptográfico, sino que simplemente se elige uno que creará el bloque:

» Todo el que quiera participar en la creación de bloques debe aportar un capital en Ethers. Este depósito es el "Stake" y es una fianza para evitar el comportamiento fraudulento de los nodos.

» Se elige el nodo que va a añadir el siguiente bloque de forma aleatoria, pero considerando entre otros factores el valor de la fianza aportada.

» Si el bloque generado no es validado por la mayoría de la red, el nodo que generó el bloque pierde la fianza.

Este sistema no solamente aporta beneficios energéticos, sino que resuelve dos problemas adicionales que existen con PoW.

El primero de ellos es la falta de escalabilidad. El número de transacciones por segundo de una red que utiliza PoW está limitado por el tiempo que se tarda en construir el bloque, elevado debido a las operaciones que tienen que hacer los mineros, y por el hecho de que el número de transacciones que contiene un bloque es finito.

El segundo problema de PoW es que es posible atacar la red blockchain si se controla el 51% de la capacidad de cálculo. Tanto en Ethereum como en Bitcoin los mineros se han agrupado en pools y este tipo de ataque sería tan sencillo como que se pusieran de acuerdo cuatro de estos pools en el caso de Bitcoin o tres en el caso de Ethereum. Los pools se crean de forma natural en PoW porque al agruparse los mineros aumentan las probabilidades de obtener beneficio. En PoS no solo no se incentiva la agrupación, sino que podría suponer un problema ya que un nodo podría perder la fianza que ha puesto si el pool actúa maliciosamente.

Adicionalmente, PoS puede adaptarse de forma sencilla a redes blockchain privadas, simplemente sustituyendo el depósito inicial por la aceptación en la red privada.

CASOS DE USO DE BLOCKCHAIN

Blockchain se ha identificado durante mucho tiempo con las criptomonedas. No sólo es la primera aplicación de blockchain sino la que hoy en día tiene mayor valor de mercado si se considera su capitalización, más de 2 billones (europeos) de dólares. Bitcoin es la criptomoneda más conocida y en la actualidad representa casi la mitad de este mercado. La segunda moneda por valor es el Ether, seguida a mayor distancia por Binance Coin.

En 2020 el valor de Bitcoin creció un 300% y los bancos de inversión han comenzado a plantearse la aplicabilidad de las criptomonedas como activos de inversión. Bancos como Citigroup, Bank of America, Morgan Stanley o Goldman Sachs ya se están posicionando en este mercado, ofreciendo servicios de análisis o incluso trading en algunos casos. También están surgiendo nuevos actores como el mercado de criptomonedas Coinbase, cuya salida a cotización en abril de 2021 fue la séptima mayor de la historia.

Además de las criptomonedas, han ido surgiendo otros campos de aplicación, tanto para empresas como para particulares. A continuación se describen varios ejemplos.

Cadenas de suministro. Al ser un registro abierto e inmutable, múltiples sectores y organizaciones están utilizando blockchain para gestionar sus cadenas de suministro. Algunos de estos sectores son alimentación, transporte de mercancías, sector del lujo y ONGs.

Alimentación. Uno de los mayores referentes del uso de blockchain en el sector alimentación es IBM Food Trust™, una red de colaboración de productores, procesadores, mayoristas, distribuidores, fabricantes, minoristas y otros, que mejora la visibilidad y responsabilidad en la cadena de suministro de alimentos. Empresas como Walmart, Nestlé o Carrefour forman parte de esta red y se apoyan en blockchain para ofrecer mayor confianza a sus clientes.

Transporte de mercancías. TradeLens, resultado de un acuerdo de colaboración entre Maersk e IBM, es una plataforma basada en blockchain orientada a la digitalización del transporte marítimo global que aglutina a todos los actores de la cadena de suministro, incluyendo propietarios de las mercancías, importadores, proveedores de transporte terrestre, puertos y terminales, transportistas oceánicos, aduanas y otras autoridades.

Sector del lujo. Un ejemplo de aplicación de blockchain al sector del lujo es la plataforma Tracr, iniciada por el grupo de joyería De Beers para establecer la trazabilidad de cada diamante. Permite añadir un certificado de identidad, basado en atributos como quilates, color y brillo, que se almacena en la cadena de bloques. De esta manera, se puede garantizar la autenticidad de las piezas y su procedencia. De la misma forma, la iniciativa TrustChain se creó para tracear y autenticar diamantes, oro y joyas en la cadena de suministro global, desde la mina hasta el comercio.

Gestión de residuos. Blockchain puede ayudar a hacer el proceso de gestión de residuos y reciclaje más transparente. La tecnología puede usarse para conectar los sistemas

de recogida con las compañías de reciclaje y sobretodo con las personas para ofrecerles la confianza de que su esfuerzo realmente se transforma en un beneficio para la sociedad o incluso para recompensarles. Un ejemplo de empresa que usa blockchain para la gestión de residuos es Plastic Bank, que fomenta el reciclaje en países en vías de desarrollo.

ONGs. Uno de los problemas a los que se enfrentan las ONGs es la desconfianza de los donantes sobre qué uso va a hacerse de sus donaciones. La trazabilidad que aporta blockchain permite dar transparencia sobre dicho uso.

Gestión de identidades. La gestión tradicional de identidades con Infraestructura de Clave Pública (Public Key Infrastructure, PKI) se basa en la existencia de Autoridades de Certificación centralizadas que firman certificados que contienen la identidad de las entidades. Según crece el número de entidades y autoridades de certificación, se incrementa la complejidad y es más probable la aparición de vulnerabilidades. Gracias a blockchain se han desarrollado aplicaciones para gestionar identidades sin depender de Autoridades de Certificación centralizadas. Esto permite simplificar el registro de identidades y tareas típicamente complejas como la actualización y revocación de credenciales.

Pagos y transferencias internacionales. En abril de 2018 el Banco Santander lanzó el primer servicio de transferencias internacionales basado en blockchain. Este servicio, llamado One Pay FX, aporta agilidad, de manera que las transferencias se realizan en menor tiempo.

Propiedad intelectual y activos digitales. Una de las aplicaciones más populares actualmente es la utilización de blockchain para representar la propiedad de activos – intelectuales, digitales o incluso físicos. Estas representaciones se materializan en tokens. Un token es una ficha criptográfica. Funciona como la ficha de un juego. Por ejemplo, igual que una ficha de Monopoly puede representar la propiedad de un coche en el juego, con blockchain un token puede representar la propiedad de una obra de arte.

La forma más habitual de generar y gestionar tokens es el estándar ERC721 que se utiliza en Ethereum. Los tokens creados con este estándar son "no fungibles" (Non Fungible Tokens, NFTs). Es decir, a diferencia de las criptomonedas que son unas iguales a otras – un bitcoin es perfectamente intercambiable por otro –, cada NFT simboliza algo diferente. Esta característica los hace idóneos para representar la propiedad de activos.

Uno de los primeros usos de NFTs fue CryptoKitties, un juego que permite comprar, coleccionar y cuidar gatitos virtuales. El juego fue tan popular que en 2017 llevó a sobrecargar la red Ethereum. En la actualidad se están utilizando NFTs para juegos y arte digital, del que hay un mercado muy activo con plataformas como rarible.com y opensea.io.

Almacenamiento de ficheros. Varias ideas de blockchain tales como la comunicación peer-to-peer, las funciones de hash o los árboles de Merkle, se han aplicado para crear una red distribuida de almacenamiento de archivos llamada Inter-Planetary File System (IPFS). A diferencia de los sistemas clásicos que acceden a un fichero a través de una URL, IPFS referencia los archivos como un hash. Las copias pueden estar distribuidas en cualquier nodo. Esto permite crear redes de distribución de contenidos (Content Delivery Networks, CDN), distribución de software o cualquier aplicación que requiera una baja latencia de acceso a ficheros.

CONCLUSIÓN

La primera aplicación de blockchain, y la más exitosa, es la criptomoneda bitcoin. No obstante, las características de descentralización, inmutabilidad y transparencia de blockchain han hecho que desde su aparición fueran muchos los que vieran en ella una tecnología disruptiva para el mundo empresarial.

En la actualidad ya son múltiples los ámbitos en los que se están aprovechando las ventajas de blockchain para la transformación de operaciones, aunque todavía quedan áreas en las que hay que avanzar. La escalabilidad de las redes blockchain, la optimización de los algoritmos de consenso o la sostenibilidad de la tecnología en su conjunto son elementos que pueden determinar el alcance futuro de blockchain.

Trabajar en estos aspectos será clave para hacer de blockchain un facilitador para la transformación profunda de sectores completos, como puede ser el caso de la cuarta revolución industrial, descrita en el artículo "Industria 4.0: La cuarta revolución industrial" de la serie UEM STEAM Essentials.

REFERENCIAS BIBLIOGRÁFICAS

» Nakamoto, S. (2008). Bitcoin: ***A peer-to-peer electronic cash system***. Recuperado de https://bitcoin.org/bitcoin.pdf

» Ramamurthy, B. (2020). ***Blockchain in action.*** Nueva York, Estados Unidos: Manning Publications.

» Merkle, R. C. (1979). ***A Certified Digital Signature.*** Crypto '89 Proceedings, pp 218-238.

» Ehrsam, W. F., Meyer, C. H. W., Smith, J. L. y Tuchman, W. L. (1978). ***Message Verification and Transmission Error Detection by Block Chaining.*** (U.S. Patent No. 4074066). U.S. Patent and Trademark Office.

» Narula, N. (2018). MIT Cryptocurrency Engineering and Design, lecture 4: ***Transactions and the UTXO Model.*** Recuperado de https://ocw.mit.edu/courses/media-arts-and-sciences/mas-s62-cryptocurrency-engineering-and-design-spring-2018/lecture-videos/lec4-transactions-and-the-utxo-model/

» Buterin, V. (2013). ***Ethereum whitepaper.*** Recuperado de https://ethereum.org/en/whitepaper/

» ***A Blockchain Platform for the Enterprise – Hyperledger Fabric.*** (2021). Recuperado de https://hyperledger-fabric.readthedocs.io

» University of Cambridge, Judge Business School. (2021). ***Cambridge Bitcoin Electricity Consumption Index.*** Recuperado de https://cbeci.org

» ***Ethereum Wiki – Proof of Stake FAQs***. Recuperado de https://eth.wiki/concepts/proof-of-stake-faqs

» ***Cryptocurrency Prices, Charts and Market Capitalizations.*** Recuperado de https://coinmarketcap.com

» Szalay, E. (2021). ***Wall Street banks diverge in views on bitcoin boom.*** Recuperado de https://www.ft.com/content/c3cb412e-e2b1-4837-a092-bcbc3eda81a1

» Staub, O. (2019). ***Revolutionizing the waste supply chain: Blockchain for social good.*** Recuperado de https://www.ibm.com/blogs/blockchain/2019/08/revolutionizing-the-waste-supply-chain-blockchain-for-social-good/

» Olson, T. (2019). ***Blockchain for assured cross-domain digital identities.*** Recuperado de https://developer.ibm.com/technologies/blockchain/articles/blockchain-for-assured-cross-domain-digital-identities/

» ***IPFS Documentation.*** (2021). Recuperado de https://docs.ipfs.io

» Sols, A. (2020). ***Industria 4.0: La cuarta revolución industrial.*** UEM STEAM Essentials

BIOGRAFÍA

Susana del Pozo es Ingeniero de Telecomunicaciones por la Universidad de Valladolid, con un MBA de la Universidad Autónoma de Madrid y más de 20 años de experiencia en el sector de tecnología.

Susana ha trabajado en empresas líderes del sector y desde su incorporación a IBM en 2006 ha ocupado diversos puestos relacionados con infraestructura tecnológica, cloud, datos e inteligencia artificial y ciberseguridad. Actualmente es la Directora de la Unidad de Seguridad de IBM para España, Portugal, Grecia e Israel y pertenece al Consejo Asesor Empresarial de la Escuela de Arquitectura, Ingeniería y Diseño de la Universidad Europea.