Una **cadena de bloques**,[1] conocida en inglés como ***blockchain***,[2][3][4][5][6] es una estructura de datos cuya información se agrupa en conjuntos (bloques) a los que se les añade metainformación relativa a otro bloque de la cadena anterior en una línea temporal para hacer un seguimiento seguro a través de grandes cálculos criptográficos. De esta forma, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques anteriores. Esta propiedad permite su aplicación en un entorno distribuido de manera que la estructura de datos *blockchain* puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información.[7]

En la práctica ha permitido, gracias a la criptografía asimétrica y las funciones de resumen o *hash*, la implementación de un registro contable (ledger) distribuido que permite soportar y garantizar la seguridad de dinero digital.[8] Siguiendo un protocolo apropiado para todas las operaciones efectuadas sobre la *blockchain*, es posible alcanzar un consenso sobre la integridad de sus datos por parte de todos los participantes de la red sin necesidad de recurrir a una entidad de confianza que centralice la información. Por ello se considera una tecnología en la que la "verdad" (estado fiable del sistema) es construida, alcanzada y fortalecida por los propios miembros; incluso en un entorno en el que exista una minoría de nodos en la red con comportamiento malicioso (nodos sybil) dado que, en teoría, para comprometer los datos, un atacante requeriría de una mayor potencia de cómputo y presencia en la red que el resultante de la suma de todos los restantes nodos combinados. Por las razones anteriores, la tecnología *blockchain* es especialmente adecuada para escenarios en los que se requiera almacenar de forma creciente datos ordenados en el tiempo, sin posibilidad de modificación ni revisión y cuya confianza pretenda ser distribuida en lugar de residir en una entidad certificadora. Este enfoque tiene diferentes aspectos:

- Almacenamiento de datos: se logra mediante la replicación de la información de la cadena de bloques
- Transmisión de datos: se logra mediante redes de pares.
- Confirmación de datos: se logra mediante un proceso de consenso entre los nodos participantes. El tipo de algoritmo de consenso más utilizado es el de prueba de trabajo en el que hay un proceso abierto competitivo y transparente de validación de las nuevas entradas llamada minería.

El concepto de cadena de bloque fue aplicado por primera vez en 2009 como parte de Bitcoin.[9]

Los datos almacenados en la cadena de bloques normalmente suelen ser transacciones (p. ej. financieras) por eso es frecuente llamar a los datos transacciones. Sin embargo, no es necesario que lo sean. Realmente podríamos considerar que lo que se registran son cambios atómicos del estado del sistema. Por ejemplo una cadena de bloques puede ser usada para estampillar documentos y asegurarlos frente a alteraciones.[10]

Historia

El criptógrafo David Chaum propuso por primera vez un protocolo similar a la cadena de bloques en su disertación de 1982 "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups".[11] En 1991, Stuart Haber y W. Scott Stornetta describieron otros trabajos sobre una cadena de bloques criptográficamente segura. y querían implementar un sistema en el que las marcas de tiempo de los documentos no pudieran ser manipuladas. En 1992, Haber, Stornetta y Dave Bayer incorporaron árboles de Merkle al diseño, lo que mejoró su eficiencia al permitir reunir varios certificados de documentos en un solo bloque.[12][13] Bajo su empresa Surety, sus hashes de certificados de documentos se han publicado en The New York Times cada semana desde 1995.[14]

El primer *blockchain* fue conceptualizado por una persona (o grupo de personas) conocida como Satoshi Nakamoto en 2008. Nakamoto mejoró el diseño de manera importante utilizando un método similar al Hashcash para sellar el tiempo de los bloques sin requerir que sean firmados por una parte de confianza e introduciendo un parámetro de dificultad para estabilizar la tasa con la que los bloques se añaden a la cadena.[12] El diseño fue implementado al año siguiente por Nakamoto como un componente central de la criptodivisa bitcoin, donde sirve como el libro de contabilidad público para todas las transacciones en la red.[9]

En agosto de 2014, el tamaño del archivo del *blockchain* de bitcoin, que contiene los registros de todas las transacciones que han ocurrido en la red, alcanzó los 20 GB (gigabytes).[15] En enero de 2015, el tamaño había crecido a casi 30 GB, y de enero de 2016 a enero de 2017, el *blockchain* de bitcoin creció de 50 GB a 100 GB de tamaño. El tamaño había superado los 200 GB a principios de 2020.[16]

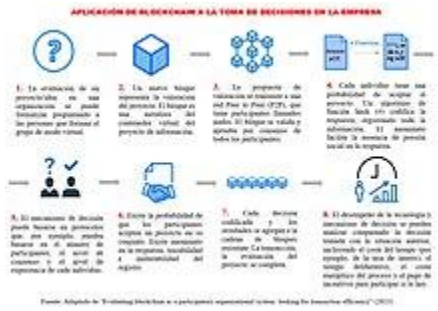
Según Accenture, una aplicación de la teoría de la difusión de las innovaciones sugiere que las cadenas de bloques alcanzaron una tasa de adopción del 13,5% dentro de los servicios financieros en 2016, alcanzando por tanto la fase de adopción temprana.[17] Los grupos comerciales de la industria se unieron para crear el Foro Global de Blockchain en 2016, una iniciativa de la Cámara de Comercio Digital.

Aplicaciones

El concepto de cadena de bloques se utiliza en los siguientes campos:

- En el campo de las criptomonedas, la cadena de bloques se usa como notario público no modificable de todo el sistema de transacciones a fin de evitar el problema de que una moneda se pueda gastar dos veces. Por ejemplo es usada en Bitcoin, Cardano, Ethereum, Dogecoin y Litecoin, aunque cada una con sus particularidades.[18]
- En el campo de las bases de datos de registro de nombres la cadena de bloques se usa para tener un sistema de notario de registro de nombres de tal forma que un nombre solo pueda ser utilizado para identificar el objeto que lo tiene efectivamente registrado. Es una alternativa al sistema tradicional de DNS. Por ejemplo es usada en Namecoin.
- Uso como notario distribuido en distintos tipos de transacciones haciéndolas más seguras, baratas y rastreables. Por ejemplo se usa para sistemas de pago,

transacciones bancarias (dificultando el lavado de dinero), envío de remesas, préstamos y en los sistemas de gestión de activos digitales puede ser usado con distintos propósitos como la toma de decisiones en las organizaciones de forma anónima.[19]



Proceso de aplicación de Blockchain en una organización para la toma de decisiones. Fuente: Adaptado de Sáenz-Royo y Fleta-Asín (2023).

- Es utilizado como base de plataformas descentralizadas que permiten soportar la creación de acuerdos de contrato inteligente entre pares. El objetivo de estas plataformas es permitir a una red de pares administrar sus propios contratos inteligentes creados por los usuarios. Primero se escribe un contrato mediante un código y se sube a la cadena de bloques mediante una transacción. Una vez en la cadena de bloques el contrato tiene una dirección desde la cual se puede interactuar con él. Ejemplos de este tipo de plataformas son Cardano, Ethereum y Ripple.
- Es utilizado en la contratación pública,[20] donde puede ayudar a incrementar la transparencia en las licitaciones.* Implementación del componente criptográfico llamado Bulletin Boards usado, entre otros, en sistemas de voto electrónico (como por ejemplo ha implementado la empresa energética española Iberdrola en su última Junta General de Accionistas), creación de registros, subastas y foros de discusión.[21][22][23][24]
- Se utiliza para el almacenamiento en la nube, por ejemplo, permite la creación de nodos en diferentes puntos geográficos que son capaces de resistir la caída de cualquier servidor.[25]
- Es utilizado para proporcionar un sistema único seguro e inmutable que supone la solución óptima para el problema de la suplantación de las identidades digitales.[25]

Clasificación

Según el acceso a los datos

Las cadenas de bloques se pueden clasificar basándose en el acceso a los datos almacenados en la misma:[10][26]

- Cadena de bloques pública: es aquella en la que no hay restricciones ni para leer los datos de la cadena de bloques (los cuales pueden haber sido cifrados) ni para enviar transacciones para que sean incluidas en la cadena de bloques. En ellas es fácil entrar y salir, son transparentes, están construidas con precaución para la operación en un

entorno no confiable. Son ideales para uso en aplicaciones totalmente descentralizadas como por ejemplo para el Internet.
- Cadena de bloques privada: es aquella en la que tanto los accesos a los datos de la cadena de bloque como el envío de transacciones para ser incluidas, están limitadas a una lista predefinida de entidades.

Ambos tipos de cadenas deben ser considerados como casos extremos pudiendo haber casos intermedios.

Según los permisos

Las cadenas de bloques se pueden clasificar basándose en los permisos para generar bloques en la misma:[10]

- Cadena de bloques sin permisos: es aquella en la que no hay restricciones para que las entidades puedan procesar transacciones y crear bloques. Este tipo de cadenas de bloques necesitan tókenes nativos para proveer incentivos que los usuarios mantengan el sistema. Ejemplos de tókenes nativos son los nuevos bitcoines que se obtienen al construir un bloque y las comisiones de las transacciones. La cantidad recompensada por crear nuevos bloques es una buena medida de la seguridad de una cadena de bloques sin permisos.
- Cadena de bloques con permisos: es aquella en la que el procesamiento de transacciones está desarrollado por una predefinida lista de sujetos con identidades conocidas. Por ello generalmente no necesitan tókenes nativos. Los tókenes nativos son necesarios para proveer incentivos para los procesadores de transacciones. Por ello es típico que usen como protocolo de consenso prueba de participación.

Posibles combinaciones de acceso y permisos

Las posibles combinaciones de ambos tipos de características son:[26]

- Cadenas de bloques públicas sin permisos. Un ejemplo de estas es Bitcoin. Como no es posible la existencia de cadenas de bloques privadas sin permisos, a estas también se las llama simplemente cadenas de bloques sin permisos.
- Cadenas de bloques públicas con permisos. Un ejemplo de estas son las cadenas laterales federadas. Estas cadenas no pueden tener ataques Sybil, por lo que en principio poseen un grado más alto de escalabilidad y flexibilidad frente a las públicas sin permisos.
- Cadenas de bloques privadas con permisos.

Esta combinación es posible ya que hay distintas formas de acceder a los datos de la cadena:[10]
- Leer las transacciones de la cadena de bloques, quizás con algunas restricciones (p. ej. un usuario puede tener acceso solo a las transacciones en las que está involucrado directamente)
- Proponer nuevas transacciones para la inclusión en la cadena de bloques.

- Crear nuevos bloques de transacciones y añadirlo a la cadena de bloques.

La última forma de acceso está restringida para cierto conjunto limitado de entidades. Sin embargo las otras dos formas de acceso no tienen por qué estar restringidas. Por ejemplo una cadena de bloques para entidades financieras sería una cadena con permisos pero podría:[10]

- Garantizar el acceso de lectura (quizá limitada) para transacciones y cabeceras de bloques para sus clientes con el objetivo de proveer una tecnológica, transparente y fiable forma de asegurar la seguridad de los depósitos de sus clientes.
- Garantizar acceso de lectura completo a los reguladores para garantizar el necesario nivel de cumplimiento.
- Proveer a todas las entidades con acceso a los datos de la cadena de bloques una descripción exhaustiva y rigurosa del protocolo, el cual debería contener explicaciones de todas las posibles interacciones con los datos de la cadena de bloques.

Según modelo de cambio de estado

Las cadenas de bloques también se pueden clasificar según el modelo de cambio de estado en la base de datos en:[27]

- Basado en el gasto de salidas de transacciones, también llamado modelo UTXO (en referencia a los UTXO de Bitcoin). En ellas cada transacción gasta salidas de transacciones anteriores y produce nuevas salidas que serán consumidas en transacciones posteriores. A este tipo de cadenas de bloques pertenecen por ejemplo las de Bitcoin, R3, Blockstream, BOSCoin y Qtum. Este enfoque tiene ventajas como:
    - En la propia estructura de la cadena existe una prueba de que nunca se puede gastar dos veces ya que cada transacción prueba que la suma de sus entradas es más grande que la suma de sus salidas.
    - Cada transacción puede ser procesada en paralelo porque son totalmente independientes y no hay conflictos en las salidas.

Sin embargo el problema de este tipo de cadenas es que solo son utilizables para aplicaciones donde cada salida es propiedad de uno y solo un individuo como por ejemplo es el caso de las monedas digitales. Una salida multipropietario sería muy lenta y no sería eficiente para aplicaciones de propósito general. Por ejemplo, supongamos un contrato inteligente que implementa un contador que puede ser incrementado. Imagina que hay algún incentivo económico para que cada nodo incremente en uno el contador, y que hay 1000 nodos activamente intentado incrementarlo. Usando este modelo de cadena de bloques tendríamos una salida con el valor del contador que sería solicitada por muchos nodos. Finalmente, un nodo tendría éxito y produciría una transacción con una nueva salida con el contador incrementado en una unidad más. El resto de los nodos estarían forzados a reintentar hasta que su transacción sea aceptada. Este sistema es muy lento e ineficiente. Esto se debe a que aun cuando se realiza la transacción se bloquea la salida, se realiza una transformación y finalmente se produce la nueva salida. Está claro que sería óptimo si se realizará todo de una sola vez y se produjera directamente el estado resultante. Además, el problema puede estar no solo en el tiempo de la transacción, sino también en el de proceso. Supongamos que el

contador tiene adjunto un buffer de 1MB cuyo valor cambia de forma determinista cada vez que el contador cambia. Se tendría que procesar 1MB cada vez que realizara una transacción

- Basado en mensajes. En este caso, la cadena de bloques representa un consenso sobre el orden de los mensajes y el estado es derivado de forma determinista a partir de estos mensajes. Este enfoque es utilizado por las cadenas de bloques de Steem y Bitshares. Por ejemplo, para implementar un contador cada usuario debería simplemente firmar un mensaje pidiendo el incremento en uno. No se necesita saber el estado actual del contador para que el mensaje sea válido. En este modelo si 1000 nodos envían la petición al mismo tiempo, el productor del bloque podría agregar todas las peticiones en un bloque y en un solo paso el contador pasaría de valer de cero a valer 1000. Una aplicación del mundo real que aprovecharía las cualidades de este modelo sería el siguiente:

Se emite una orden de compra de productos financieros indicando un precio máximo y un volumen concreto. A partir de ahí hay una competición sobre esa salida entre los participantes que quieren la solicitud al mismo tiempo. Supongamos que se desea realizar la transacción de forma que sea lo más beneficiosa posible realizando una subasta a la baja para que la solicitud compre activos por el menor precio.[27]

Infografía con algoritmos matemáticos detrás de blockchain, así como qué técnica nos garantiza cada característica.

Características clave de la red blockchain

- Consenso: Para que una transacción sea válida, todos lo participante (o la mayoría) deben de estar de acuerdo con su validez.[28]
- Procedencia: Los participantes saben de donde viene el eslabón y como ha cambiado su propietario con el tiempo.
- Inmutabilidad: Ningún participante puede modificar la lista de registros una vez que se haya guardado en la cadena. Si una transacción es errónea, se debe hacer una nueva para corregirla, tras lo cual ambas transacciones serán visibles.
- Finalidad: Un eslabón dirige a una sola cadena para determinar la propiedad de un activo o el final de una transacción.[29]

Cadena lateral

Una cadena lateral, en inglés *sidechain*, es una cadena de bloques que valida datos desde otra cadena de bloques a la que se llama principal. Su utilidad principal es poder aportar funcionalidades nuevas, las cuales pueden estar en periodo de pruebas, apoyándose en la confianza ofrecida por la cadena de bloques principal.[30][31] Las cadenas laterales funcionan de forma similar a como hacían las monedas tradicionales con el patrón oro.[32]

Un ejemplo de cadena de bloques que usa cadenas laterales es Lisk.[33] Debido a la popularidad de Bitcoin y la enorme fuerza de su red para dar confianza mediante su algoritmo de consenso por prueba de trabajo, se quiere aprovechar como cadena de bloques principal y construir cadenas laterales vinculadas que se apoyen en ella. Una cadena lateral vinculada es una cadena lateral cuyos activos pueden ser importados desde y hacia la otra cadena. Este tipo de cadenas se puede conseguir de dos formas:[31]

- Vinculación federada, en inglés *federated peg*. Una cadena lateral federada es una cadena lateral en la que el consenso es alcanzado cuando cierto número de partes están de acuerdo (confianza semicentralizada). Por tanto tenemos que tener confianza en ciertas entidades. Este es el tipo de cadena lateral Liquid, de código cerrado, propuesta por Blockstream.[34]
- Vinculación SPV, en inglés *SPV peg* donde SPV viene de *simplified payment verification*. Usa pruebas SPV. Esencialmente una prueba SPV está compuesta de una lista de cabeceras de bloque que demuestran prueba de trabajo y una prueba criptográfica de que una salida fue creada en uno de los bloques de la lista. Esto permite a los verificadores chequear que cierta cantidad de trabajo ha sido realizada para la existencia de la salida. Tal prueba puede ser invalidada por otra prueba demostrando la existencia de una cadena con más trabajo la cual no ha incluido el bloque que creó la salida. Por tanto no se requiere confianza en terceras partes. Es la forma ideal. Para conseguirla sobre Bitcoin el algoritmo tiene que ser modificado y es difícil alcanzar el consenso para tal modificación. Por ello se usa con bitcóin la vinculación federada como medida temporal

Aspectos jurídicos de las cadenas de bloques y Bitcoin

El uso de una cadena de bloques en la práctica ha permitido resolver dos problemas relacionados con el intercambio de activos sin una entidad certificadora de confianza:

1. Evitar el problema del doble gasto, es decir evita la falsificación y que una misma moneda pueda ser gastada dos veces.
2. Conseguir la descentralización de los pagos electrónicos ya que se garantiza la realización segura de pagos y cobros directos entre particulares por vía electrónica.[35]

Además, la confianza es otra de las características intrínsecas del sistema. Desde el punto de vista jurídico el bitcoin sería un bien patrimonial, privado, incorporal, digital, en forma de unidad de cuenta, creado mediante un sistema informático y utilizado como medida común de valor por acuerdo de los usuarios del sistema. Es un bien mueble, fungible, identificable e irrepetible pero divisible. Pero no es dinero, no es dinero electrónico ni tiene valor mobiliario, se trataría de «bienes patrimoniales que son tomados como medida común de valor en sistemas de intercambio económico, cerrados, cooperativos y descentralizados, ajenos al dinero fiduciario estatal, y basados en la confianza y acuerdo de los usuarios del sistema». Para González Granado el bitcoin sin regulación no se constituirá en una moneda de uso general como medio de pago.[3536]

Ética en las cadenas de bloques

Seguridad y confianza

La ética de la tecnología blockchain se enfoca en su capacidad para proporcionar seguridad y confianza a los usuarios,[37] gracias a su transparencia y su imposibilidad de modificar los datos una vez que se han registrado en la cadena de bloques.

En primer lugar, la transparencia de la tecnología blockchain se debe a que todas las transacciones y operaciones realizadas en la red son públicas y visibles para cualquier usuario. Esto implica que los datos son accesibles y verificables por cualquier persona, lo que aumenta la confianza de los usuarios en la integridad del sistema y la transparencia en las transacciones.[38]

Además, la tecnología blockchain es inmutable, lo que significa que los datos una vez registrados en la cadena de bloques no pueden ser alterados o eliminados. Esto garantiza que la información almacenada en la cadena de bloques sea confiable y precisa, y que no haya manipulación de datos por parte de terceros.[39]

La tecnología blockchain se puede considerar ética ya que protege la privacidad y la integridad de los datos de los usuarios, evitando fraudes y robos de información, lo que fomenta la confianza en la red y en las operaciones realizadas en ella.

Lucha contra la falsificación

El blockchain, una tecnología de registro distribuido,[40] se ha establecido como una herramienta valiosa para combatir la falsificación y el fraude. Una de las características clave del blockchain es su inmutabilidad de los datos, lo que significa que una vez que se registra una transacción en la cadena de bloques, no se puede alterar o eliminar. Esto garantiza que los datos y transacciones sean auténticos y fiables, lo que a su vez conduce a una mayor eficiencia y seguridad en los procesos de negociación y en la cadena de suministro empresarial.[41]

En la lucha contra la falsificación y el fraude, el blockchain también ha demostrado ser útil en la protección de los derechos de autor, como obras de arte y medicamentos. Al registrar la información de estos productos en la cadena de bloques, se puede garantizar su autenticidad y proteger a los consumidores de posibles fraudes.[42]

Se podría decir que el blockchain ofrece una solución ética para abordar la falsificación y el fraude al garantizar la autenticidad y fiabilidad de los datos y transacciones. Esto tiene un impacto positivo en la sociedad al brindar mayor seguridad y protección a los consumidores y empresas.

Responsabilidad y gobernanza

La gobernanza en blockchain se refiere a la forma en que se toman decisiones y se resuelven conflictos dentro de la red. En general, debe ser justa, transparente y democrática, para garantizar la participación equitativa de los usuarios y la toma de decisiones en beneficio del bien común.[43]

Existen diferentes modelos de gobernanza en blockchain.[44] Uno de los más comunes es el modelo descentralizado, en el que las decisiones se toman colectivamente por los usuarios de la red. Cada usuario tiene un voto y las decisiones se toman por mayoría, lo que promueve la participación democrática y la igualdad de todos los usuarios.

Otro modelo es el delegado, en el que un grupo de usuarios es elegido para tomar decisiones en nombre de la comunidad. Los usuarios eligen a los delegados por votación y estos tienen la responsabilidad de tomar decisiones en beneficio del bien común. La transparencia en la toma de decisiones es esencial para garantizar que los delegados actúen en beneficio de la comunidad y no en sus propios intereses.[45]

En algunos casos, la gobernanza en blockchain puede ser automatizada mediante el uso de contratos inteligentes. Estos programas se ejecutan automáticamente en la red y siguen ciertas reglas para tomar decisiones. Por ejemplo, pueden utilizarse para distribuir recompensas a los nodos que realizan tareas específicas. Este modelo promueve la transparencia y la imparcialidad en la toma de decisiones.

Impacto medioambiental

La ética ambiental del blockchain se centra en los efectos ambientales de la tecnología blockchain en la gestión y compartición de información. El blockchain puede reducir el impacto medioambiental mediante la gestión eficiente de la energía renovable.[46] Sin embargo, la

minería de criptomonedas conlleva un alto consumo de energía,[47][48] lo que plantea preocupaciones éticas y ambientales. Además, la producción y eliminación de los equipos utilizados para la minería también son problemáticas.[49] Se necesitan soluciones más sostenibles para abordar el impacto ambiental del blockchain y se deben considerar las implicaciones éticas al utilizar la tecnología para otros fines.