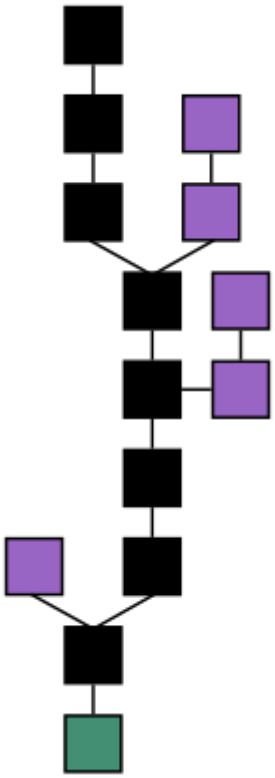
Cadena de bloques

Una **cadena de bloques**[1] o **cadena articulada**, conocidas en inglés como ***blockchain***,[2][3][4][5][6] es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade metainformación relativa a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas la información contenida en un bloque sólo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en 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 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 confiable del sistema) es construída, 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 distribuída en lugar de residir en una entidad certificadora. Este enfoque tiene diferentes aspectos:



Formación de una cadena de bloques. La cadena mayor (negra) consta de la serie de bloques más larga del bloque de génesis (verde) al bloque actual. Los bloques huérfanos (púrpura) existen fuera de la cadena mayor

- 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 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.

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.[9]

Índice

Aplicaciones

El concepto de cadena de bloques se usa 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, Ethereum, Dogecoin y Litecoin, aunque cada una con sus particularidades.[10]
- En el campo de las bases de datos de registro de nombres la cadena de bloques es usada 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 lossistemas de gestión de activos digitalespuede ser usado condistintos propósitos
- 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 soEthereum y Ripple.
- Implementación del componente criptográfico llamado Bulletin Boards usado, entre otros, en sistemas de voto electrónico, creación deregistros, subastas y foros de discusión.[11] [12] [13]

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.[9] [14]

- 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:[9]

- 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 consensoprueba de participación

Posibles combinaciones de acceso y permisos

Las posibles combinaciones de ambos tipos de características son:[14]

- 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:[9]

  - 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:[9]

  - 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:[15]

- 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 nodos estarían forzados a reintentar hasta que su transacción sea aceptada. Este sistema es muy lento e ineficiente. Esto es debido a que un cuando se realiza la transacción se bloquea la salida, se realiza una transformación y finalmente se produce la nueva salida. Esta claro que sería mucho más óptimo si se realizara 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 determinísta 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 la 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 participante 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.[15]

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.[16] [17] Las cadenas laterales funcionan de forma similar a como hacían las monedas tradicionales con el patrón oro.[18]

Un ejemplo de cadena de bloques que usa cadenas laterales es Lisk.[19] 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 las siguiente formas[17]:

- 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.[20]
- 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.[21]

Además, la confianza es otra de las característica intrínseca del sistema. Desde el punto de vista jurídico el bitcóin 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 bitcóin sin regulación no se constituirá en una moneda de uso general como medio de pago.[21] [22]

Bibliografía

- *La revolución blockchain*, Don Tapscott & Alex Tapscott. 2016. Deusto.
- *An Integrated Reward and Reputation Mechanism for MCS Preserving Users' Privacy*. Cristian Tanas, Sergi Delgado-Segura, Jordi Herrera-Joancomartí. 4 de febrero de 2016. Data Privacy Management, and Security Assurance. pp 83-99
- *La Revolución de la tecnología de Cadenas de Bloques en la economía: Impacto en los distintos Sectores Económicos*, Santiago Moreno Ismael. 31 de marzo de 2017. EAE...

Enlaces externos

- The API Hour: Blockchain Day (evento completo) BBVA Innovation Center. 21 de abril de 2016
- Retos del BitCoin y de la Blockchain, I Jornadas Notariado TIC, 2016 - Presentación

Referencias

1. «cadena de bloques, mejor que blockchain» (http://www.fundeu.es/recomendacion/cadena-de-bloques-mejor-que-blockchain/). Consultado el 27 de diciembre de 2017.
2. Economist Staff (31 de octubre de 2015). «Blockchains: The great chain of being sure about things» (http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable) *The Economist*. Consultado el 18 de junio de 2016. «[Subtitle] The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.»
3. Morris, David Z. (15 de mayo de 2016). «Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting» (http://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/) *Fortune (revista)*. Consultado el 23 de mayo de 2016
4. Popper, Nathan (21 de mayo de 2016). «A Venture Fund With Plenty of Virtual Capital, but No Capitalist» (https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html?_r=1). *New York Times*. Consultado el 23 de mayo de 2016
5. Brito, Jerry & Castillo, Andrea (2013). «Bitcoin: A Primer for Policymakers» (http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf). Fairfax, VA: Mercatus Center, George Mason University. Consultado el 22 de octubre de 2013
6. Trottier, Leo (18 de junio de 2016). «original-bitcoin» (https://github.com/trottier/original-bitcoin/blob/master/src/main.h#L795-L803) (self-published code collection). github. Consultado el 18 de junio de 2016. «This is a historical repository of Satoshi Nakamoto's original bit coin sourcecode».
7. «Blockchain» (http://www.investopedia.com/terms/b/blockchain.asp). *Investopedia*. Consultado el 19 de marzo de 2016. «Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system.»
8. Orcutt, Mike (1 de marzo de 2018). «Ethereum's smart contracts are full of holes» (http://archive.today/QjwRx) (htnl). TechnologyReview (en inglés). Archivado desde el original (https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/) el 6 de marzo de 2018. Consultado el 18 de abril de 2018. «A blockchain is essentially a shared accounting ledger that uses cryptography and a network of computers to track assets and secure the ledger from tampering.»
9. Public versus Private Blockchains. Part 1 (http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf) Public versus Private Blockchains. Part 2 (http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf). BitFury Group in collaboration with Jeff Garzik. Octubre 2015
10. «Particularidades Desarrollo Blockchain» (http://blog.coinfabrik.com/overview-of-blockchain-technologies/) Consultado el 7 de marzo de 2017
11. Blockchains and bulletin boards (https://nvotes.com/blockchains-and-bulletin-boards/) David Ruescas. Mayo de 2016. nvotes.com
12. Efficient Asynchronous Accumulators for Distributed PKI (https://eprint.iacr.org/2015/718.pdf). Leonid Reyzin et al. Security and Cryptography for Networks: 10th International Conference, SCN 2016. Springer International 2016
13. The append-only web bulletin board (https://pdfs.semanticscholar.org/c0b1/9e1a29f5c2e415e086b48620a177c5a4cf3a.pdf). James Heather et al. Formal Aspects in Security and Trust: 5th International Workshop. FAST 2008. Prentice Hall 2008
14. Digital Assets on Public Blockchains (http://bitfury.com/content/5-white-papers-research/bitfury-digital_assets_on_public_blockchains-1.pdf) BitFury Group. Marzo 2016
15. Blockchain UTXO Model is a Dead End for General Purpose Applications (https://steemit.com/blockchain/@dantheman/blockchain-utxo-model-is-a-dead-end-for-general-purpose-applications) dantheman. 26 de marzo de 2017

16. La revolución de la tecnología de las cadenas de bloques y su impacto en los sectores económicos. Ismael Santiago Moreno. Profesor Doctor de Finanzas. Universidad de Sevilla octubre 2016
17. Enabling Blockchain Innovations with Pegged Sidechains (https://blockstream.com/sidechains.pdf) Adam Back et ali. 2014
18. Cadenas laterales: el gran salto adelante (http://elbitcoin.org/cadenas-laterales-el-gran-salto-adelante/) Majamalu el 11 abril, 2014 en Economía, Opinión
19. Lisk libera la primera criptomoneda modular con cadenas laterales (http://criptonoticias.com/mercados/lisk-libera-primera-criptomoneda-modular-cadenas-laterales/#axzz4Rfsp3ieu) Bitcoin PR Buzz. Mayo 2016
20. Liquid Recap and FAQ (https://blockstream.com/2015/11/02/liquid-recap-and-faq.html) Johnny Dilley. Noviembre de 2015
21. «NotarTIC|Retos| Bitcoin | Blockchain | Taller de derechos» (http://tallerdederechos.com/notartic-i-retos-del-bitcoin-y-de-la-blockchain/) *tallerdederechos.com*. Consultado el 2018-04-05
22. «"Blockchain no va a acabar con el notariado, es un instrumento que tenemos que poner a nuestro servicio"» (https://www.territoriobitcoin.com/blockchain-no-va-a-acabar-con-el-notariado-es-un-instrumento-que-tenemos-que-poner-a-nuestro-servicio/) *Territorio Bitcoin, Información independiente de Bitcoin Blockchain y Fintech en España*. 2016-11-23. Consultado el 2018-04-05
