

Alfonso González

Consultor cuantitativo en Afi, Analistas Financieros Internacionales

Pocas palabras han recorrido tanto camino en tan poco tiempo como *blockchain*. En apenas una década ha pasado de ser una curiosidad técnica conocida por un puñado de criptógrafos a convertirse en bandera de inversores, titular de prensa y promesa recurrente de gobiernos y consejos de administración. Por el camino se ha cargado de significados contradictorios: para unos, es la base de una nueva economía sin intermediarios; para otros, poco más que el envoltorio tecnológico de una burbuja especulativa. Conviene, antes de entrar en debates sobre su impacto, detenerse en una pregunta más modesta y útil: ¿qué es, exactamente, una cadena de bloques? Este artículo intenta responderla sin dar por supuesto ningún conocimiento previo y, sobre todo, sin recurrir a la jerga que tantas veces sustituye a la explicación.

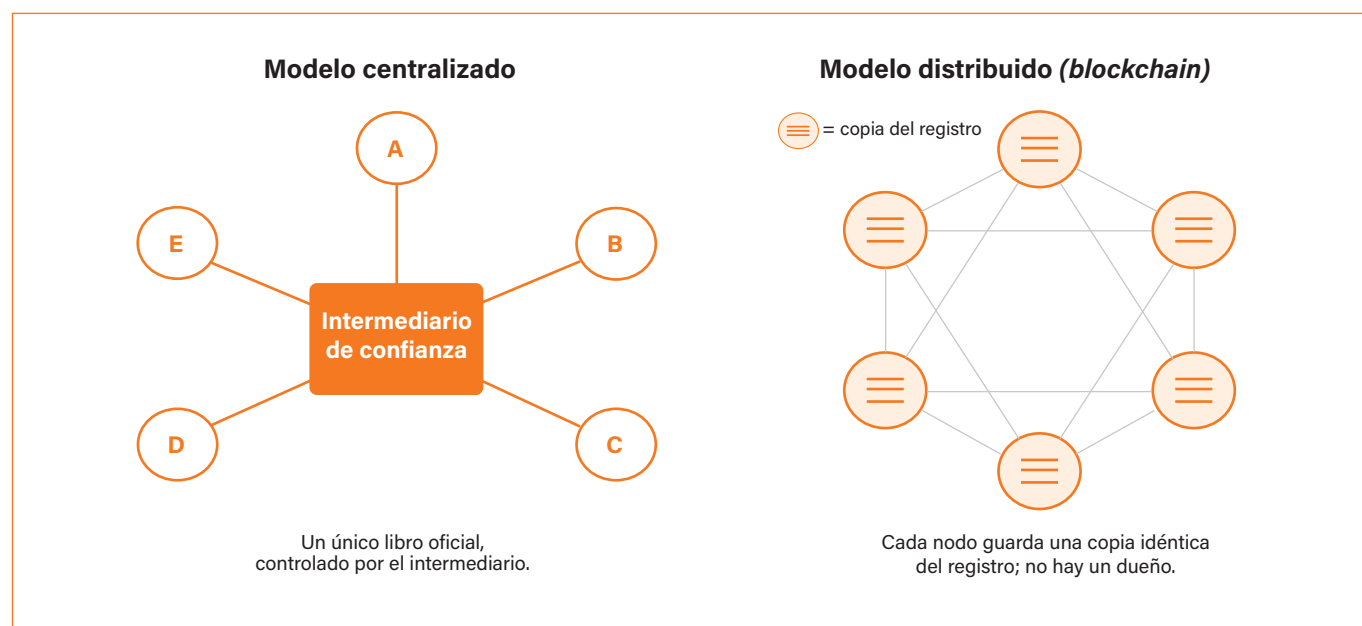
La respuesta corta es que una *blockchain* es, ante todo, una forma de llevar un registro compartido y fiable —una contabilidad, una lista de quién tiene qué o de qué ha ocurrido— sin que nadie esté al mando de él. Todo lo demás, las criptomonedas, los tokens o los contratos inteligentes, son aplicaciones construidas sobre esa idea. Y para juzgar con criterio el resto de este número conviene entender primero ese cimiento.

El problema de fondo: confiar sin intermediario

Imaginemos algo tan cotidiano como una transferencia bancaria. Cuando enviamos dinero a otra persona no entregamos físicamente nada: simplemente, nuestro banco resta una cifra de nuestra cuenta y la suma a la del destinatario. Confiamos en que el apunte es correcto porque confiamos en el banco, una entidad central que mantiene el libro de cuentas oficial y que responde ante un supervisor. El sistema funciona porque existe un tercero en quien todos confiamos.

Esa figura del intermediario de confianza —el banco, el registro de la propiedad, el notario, la plataforma que custodia nuestros datos— está presente en casi todos los intercambios de la economía moderna. Aporta orden y seguridad, pero también tiene un coste: cobra por su servicio, puede equivocarse, puede sufrir un ataque, puede excluir a quien no le interese y, en último término, concentra mucho poder sobre la información.

Figura 1. En un sistema centralizado, el registro lo custodia un intermediario; en una blockchain, lo comparten en copias idénticas todos los nodos de la red. Fuente: Afi



La pregunta que dio origen a *blockchain* fue precisamente esa: ¿es posible mantener un registro en el que todos confíen sin necesidad de una autoridad central que lo custodie? El reto tiene incluso un nombre propio, el problema del doble gasto. En el mundo físico, si entrego un billete dejo de tenerlo y no puedo gastarlo dos veces; pero un archivo digital se copia con un clic. ¿Cómo impedir que alguien gaste la misma moneda digital dos veces si no hay un banco que lleve la cuenta? La solución que propuso en 2008 un autor —o grupo— bajo el seudónimo de Satoshi Nakamoto, en el breve documento que dio lugar a Bitcoin,¹ no fue inventar un intermediario mejor, sino prescindir de él y repartir su función entre miles de participantes.

Un libro de cuentas que todos guardan

El primer ingrediente de una cadena de bloques es, por tanto, un libro de contabilidad compartido. En lugar de existir una única copia oficial en manos de una entidad, existen muchas copias idénticas distribuidas por la red, una en cada nodo, es decir, en cada ordenador que participa. De ahí el término técnico que mejor define a esta tecnología: registro distribuido.

La diferencia con un sistema tradicional es profunda. Si el libro lo guarda un solo banco y ese banco falla, miente o sufre un ataque, el registro entero está en riesgo. Si lo guardan a la vez miles de nodos repartidos por el mundo, manipularlo exige ponerse de acuerdo —o engañar— a una mayoría de ellos al mismo tiempo, algo mucho más difícil. La información deja de tener un único punto de control y, con él, un único punto de fallo.

Pero un libro repartido entre desconocidos plantea de inmediato dos problemas prácticos. El primero: ¿cómo evitar que cualquiera reescriba a su antojo el historial? El segundo: ¿cómo logran ponerse de acuerdo todas esas copias sobre cuál es la versión correcta? *Blockchain* resuelve el primero con criptografía y el segundo con lo que se conoce como mecanismo de consenso. Conviene verlos por separado.

Bloques encadenados: por qué cuesta tanto falsificarlo

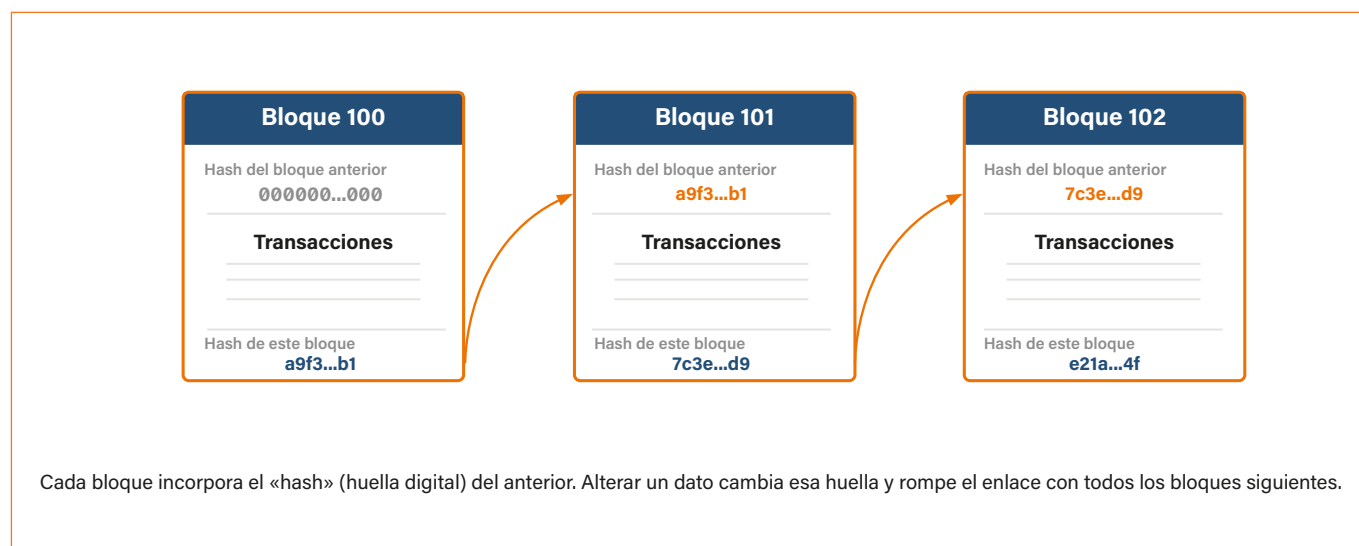
Las anotaciones del registro —en Bitcoin, las transacciones— no se añaden de una en una, sino agrupadas en lotes llamados bloques. Cada cierto tiempo se cierra un bloque con las operaciones recientes y se enlaza al anterior, formando una cadena que crece de manera continua: la cadena de bloques que da nombre a la tecnología.

Lo ingenioso es cómo se enlazan. Cada bloque incluye una especie de huella digital del bloque que le precede. Esa huella se obtiene mediante una función matemática llamada «función *hash*», que merece una explicación porque es el verdadero pegamento del sistema. Una función *hash* toma cualquier cantidad de información —una palabra, un contrato, todo un bloque de transacciones— y la transforma en una cadena de caracteres de longitud fija, una especie de resumen único. Tiene tres propiedades clave para lo que nos ocupa: a una misma información le corresponde siempre el mismo resumen; un cambio mínimo en la información, una coma o un céntimo, produce un resumen completamente distinto; y, por último, es prácticamente imposible recorrer el camino inverso y deducir la información original a partir del resumen.

Como cada bloque contiene el *hash* del anterior, todos quedan encadenados de forma que el orden y el contenido quedan sellados. Si alguien intentara alterar una transacción de un bloque antiguo —digamos, para regalarse unas monedas—, el *hash* de ese bloque cambiaría; al cambiar, dejaría de coincidir con el que figura anotado en el bloque siguiente, y ese desajuste se propagaría como una ficha de dominó por toda la cadena posterior. El fraude no pasaría desapercibido: saltaría a la vista de todos los nodos. Para que el engaño cuadrara, el atacante tendría que rehacer ese bloque y todos los que viniesen después, y hacerlo más deprisa que el resto de la red trabajando junta. Como veremos, eso es deliberadamente muy costoso.

1. Nakamoto, S. (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. Documento fundacional, disponible en bitcoin.org.

Figura 2. Los bloques se enlazan mediante huellas criptográficas (hashes): alterar un dato rompe la cadena y delata la manipulación. Fuente: Afi



Conviene subrayar aquí un matiz que suele perderse en las versiones simplificadas: una cadena de bloques no es infalsificable, como a veces se dice, sino resistente a la manipulación y, sobre todo, evidente ante ella. No es que no se pueda alterar; es que alterarla sin que nadie lo note resulta extraordinariamente difícil y caro.

Llaves, firmas y propiedad

Queda por resolver quién puede mover qué. Si no hay un banco que compruebe nuestra identidad con una contraseña, ¿cómo se demuestra que una orden de pago la da realmente el dueño de los fondos? Aquí entra el segundo gran pilar criptográfico: la criptografía de clave pública.²

Cada usuario dispone de un par de claves vinculadas matemáticamente. Una es la clave pública, que funciona como un número de cuenta: puede compararse libremente y sirve para que otros nos envíen fondos. La otra es la clave privada, un secreto que solo conoce su titular y que actúa como una firma infalsificable. Cuando ordenamos una transacción, la firmamos con la clave privada, y cualquiera en la red puede comprobar, usando la clave pública correspondiente, que esa firma es auténtica, todo ello sin que el secreto llegue a revelarse jamás. Es el equivalente digital de

una rúbrica que cualquiera puede verificar, pero nadie puede imitar.

De aquí se desprende una consecuencia que conviene grabar a fuego, porque está detrás de buena parte de los disgustos en este mundo: en una *blockchain*, el control de los fondos reside en quien posee la clave privada. No hay un servicio de atención al cliente que restituya una contraseña perdida ni que revierta un pago enviado por error. De ahí la máxima que repiten los más veteranos: si no son tus llaves, no son tus monedas. La autonomía que ofrece esta tecnología viene acompañada de una responsabilidad, la custodia de las claves, que el sistema bancario tradicional asumía por nosotros.

¿Quién decide qué es verdad? El consenso

Tenemos ya un libro repartido en miles de copias y sellado criptográficamente. Falta lo más difícil: que toda la red, formada por participantes anónimos que no se conocen ni tienen por qué fiarse entre sí, se ponga de acuerdo sobre cuál es la versión válida del registro cada vez que se añade un bloque. A las reglas que permiten alcanzar ese acuerdo sin una autoridad central se las llama «mecanismos de consenso», y son, probablemente, la pieza más original de todo el invento.

El primero y más conocido es la prueba de trabajo, el que utiliza Bitcoin. Funciona como una competición: los nodos llamados mineros pugnan por resolver un problema matemático que solo puede abordarse por ensayo y error, probando millones de combinaciones por segundo. El primero que da con la solución gana

2. La criptografía de clave pública es muy anterior a *blockchain*: la introdujeron Whitfield Diffie y Martin Hellman en 1976, y es la misma familia de técnicas que hoy protege, entre otras cosas, las conexiones seguras de internet.

el derecho a añadir el siguiente bloque y recibe una recompensa en monedas. Hallar la solución exige una enorme cantidad de cálculo —y, por tanto, de electricidad—, pero comprobar que es correcta resulta inmediato para los demás. Esa asimetría es la clave de su seguridad: como reescribir la historia obligaría a rehacer todo ese trabajo a una velocidad inalcanzable, el fraude se vuelve económicamente absurdo. La honradez sale más a cuenta que el ataque.

Esa seguridad tiene, sin embargo, una factura energética considerable, que es uno de los grandes reproches que se hacen a este mecanismo de consenso y que otros artículos de este Dossier abordan en detalle. Según las estimaciones del centro especializado de la Universidad de Cambridge, la red Bitcoin consumía

en 2025 del orden de 138 teravatios-hora al año, una cifra comparable al consumo eléctrico de un país de tamaño medio.³

En parte como respuesta a ese problema surgió la principal alternativa, la prueba de participación, que la red Ethereum adoptó en 2022. En lugar de competir gastando electricidad, los participantes depositan como garantía una parte de sus propias monedas para optar a validar bloques. Si actúan con honradez reciben una recompensa y, si intentan hacer trampa, pierden lo depositado. El incentivo deja de ser gana quien más calcula, para pasar a quien más se juega, más motivos tiene para no engañar. El cambio fue drástico también en lo ambiental: la transición de Ethereum redujo su consumo energético en más de un 99%.⁴

Tabla 1. Las dos grandes familias de mecanismos de consenso. Fuente: Afí

	Prueba de trabajo (PoW)	Prueba de participación (PoS)
Cómo se compite	Resolviendo cálculos (minería)	Depositando monedas en garantía
Recurso clave	Potencia de cálculo y electricidad	Capital inmovilizado (<i>stake</i>)
Coste energético	Muy alto	Muy bajo
Ejemplo destacado	Bitcoin	Ethereum (desde 2022)

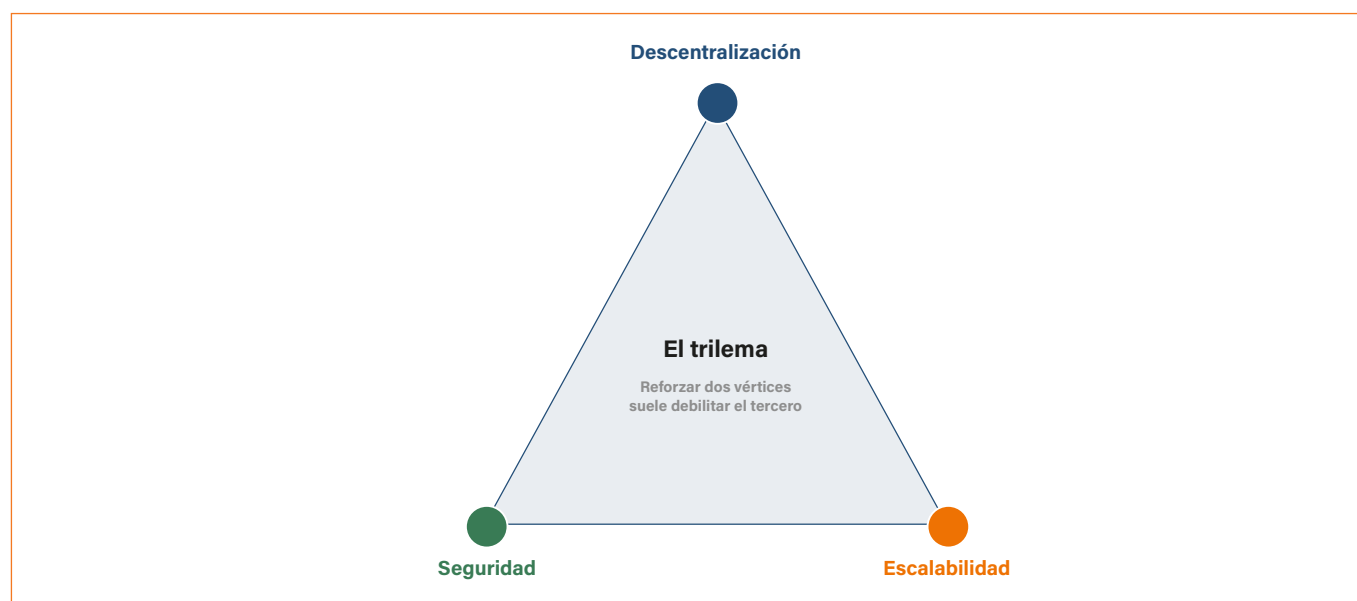
Existen otros muchos mecanismos, pero estas dos familias bastan para captar la idea esencial: como no hay un árbitro central, el acuerdo se consigue haciendo que comportarse con honradez sea siempre más rentable que intentar engañar. La seguridad de una cadena de bloques no descansa tanto en la bondad de sus participantes como en un cuidadoso diseño de incentivos.

No hay magia: los compromisos del diseño

Llegados a este punto conviene desinflar una expectativa muy extendida, la de que *blockchain* es una tecnología superior a cualquier base de datos y útil para casi todo. No lo es. Toda esa maquinaria —miles de copias del registro, sellado criptográfico, competición por el consenso— tiene un precio en eficiencia.

3. Cambridge Centre for Alternative Finance, *Cambridge Digital Mining Industry Report* (2025). Otras fuentes ofrecen cifras más altas, pero todas sitúan el consumo en el rango de un país de tamaño medio.
4. Ethereum Foundation, sobre la actualización conocida como *The Merge* (septiembre de 2022).

Figura 3. El trilema de la blockchain: descentralización, seguridad y escalabilidad son difíciles de maximizar a la vez. Fuente: Afi



El más visible es la velocidad. Una cadena de bloques pública es, por diseño, mucho más lenta que un sistema centralizado. La red Bitcoin procesa apenas un puñado de transacciones por segundo y Ethereum, unas pocas decenas. La red de una tarjeta como Visa maneja, en cambio, miles.⁵ La razón es sencilla: que miles de nodos repartidos por el planeta tengan que recibir, verificar y almacenar cada operación es inevitablemente más costoso que anotarla en el servidor de una sola empresa.

Los ingenieros del sector resumen esta tensión en lo que llaman el trilema de la *blockchain*, una idea popularizada por uno de los fundadores de Ethereum.⁶ Sostiene que un sistema de este tipo persigue tres propiedades deseables —descentralización, que no dependa de unos pocos; seguridad, que resista ataques; y escalabilidad, que sea rápido y barato a gran escala—, pero que en la práctica resulta muy difícil maximizar las tres a la vez: reforzar dos suele ir en detrimento de la tercera. Bitcoin y Ethereum priorizan la descentralización y la seguridad, y pagan el precio en velocidad; otras redes más veloces lo consiguen, a menudo, concentrando el control en menos manos.

Esa dificultad de alcanzar un equilibrio entre las tres propiedades no es un defecto que vaya a desaparecer, sino que se trata de una consecuencia estructural de querer prescindir de la autoridad central. Buena parte de la innovación reciente del sector consiste, precisamente, en buscar atajos para ganar velocidad/escalabilidad sin renunciar del todo a las otras dos propiedades.

No todas las cadenas de bloques son iguales

Hasta aquí hemos descrito cadenas públicas: redes abiertas en las que cualquiera puede participar, leer el registro e incluso validar bloques, como Bitcoin o Ethereum. Pero existe otra familia, las cadenas privadas o permissionadas, en las que solo intervienen entidades autorizadas: un grupo de bancos, las administraciones de un consorcio o las empresas de una cadena de suministro.

La distinción importa porque cambia la naturaleza del sistema. Una red permissionada gana velocidad y control —y cumple más fácilmente con la normativa— a costa de renunciar a la descentralización que daba sentido al diseño original. Conserva ventajas como el sellado criptográfico y la existencia de un registro compartido entre varias partes, pero reintroduce, en buena medida, la figura de unos pocos administradores de confianza. Muchas de las aplicaciones empresariales y buena parte de los proyectos de moneda digital de banca central que se mencionan en esta publicación pertenecen a esta categoría. No es mejor ni peor: es una herramienta distinta para un problema distinto.

5. A título orientativo, Bitcoin procesa del orden de siete transacciones por segundo y Ethereum entre quince y treinta en su capa base; Visa gestiona de media unos pocos miles, aunque su capacidad teórica es muy superior. Las cifras varían según la fuente y la forma de medirlas.

6. La formulación del «trilema» se atribuye a Vitalik Buterin, cofundador de Ethereum; su propuesta original sobre la red puede consultarse en el llamado *Ethereum Whitepaper* (2013).

Qué es y qué no es *blockchain*

Conviene, para terminar, separar la tecnología de la mitología que la rodea. Una cadena de bloques no es sinónimo de criptomoneda: es la infraestructura sobre la que las criptomonedas funcionan, pero también sirve para otros fines. No garantiza el anonimato: en redes como Bitcoin las transacciones son públicas y rastreables, aunque las identidades figuren bajo seudónimo. No es imposible de atacar: lo muy resistente es el registro en sí, pero las plataformas, las aplicaciones y, sobre todo, la custodia de las claves, siguen siendo vulnerables, como recuerdan los frecuentes robos y estafas que otros capítulos de este número analizan. Y, desde luego, no es la mejor solución para cualquier problema.

¿Cuándo aporta valor de verdad? A grandes rasgos, cuando se cumplen tres condiciones: que varias partes que no se fían plenamente entre sí necesiten compartir un mismo registro; que convenga que ese registro sea difícil de manipular y quede a la vista de todos; y

que no exista —o no se desee— una autoridad central en la que todos confíen. Si falta alguna de ellas, una base de datos tradicional bien gestionada suele ser más barata, más rápida y perfectamente adecuada. Reconocer dónde encaja esta tecnología y dónde no es la mejor vacuna contra el doble riesgo de la euforia y del rechazo automático.

Eso es, despojada de adornos, una *blockchain*: un registro compartido, sellado mediante criptografía y mantenido al día por una red que se pone de acuerdo siguiendo unas reglas en lugar de obedecer a un jefe. Una idea, en el fondo, sencilla, aunque su ejecución sea sofisticada. Sobre este cimiento se levantan las aplicaciones, las promesas y los riesgos que recorren el resto de este número, desde los activos tokenizados y las monedas digitales hasta sus impactos sociales y ambientales. Entender el cimiento es el primer paso para juzgar con criterio todo lo demás.⁷ ■

7. Para una introducción accesible pero rigurosa, véase Narayanan, A., Bonneau, J., Felten, E., Miller, A. y Goldfeder, S. (2016): *Bitcoin and Cryptocurrency Technologies*, Princeton University Press.