# BLOCKCHAIN: ¿DÓNDE RADICA SU VALOR?



• David Díaz, Cristóbal Pereira, Rodrigo Sainz

Corría el año 2008, plena crisis financiera, cuando un misterioso Satoshi Nakamoto[1] publicó un paper en internet sobre una nueva lógica de intercambio de unidades de valor; lo llamó Bitcoin. Con esta nueva tecnología, no habría necesidad de pasar por instituciones financieras para confirmar las transacciones (sumas y restas en un registro de unidades), sino que serían confirmadas públicamente en internet, a través de una lógica de mercado.

En palabras sencillas, propuso democratizar y distribuir la tarea de confirmación y registro de transacciones, a quien quisiera participar del nuevo sistema, quienes serían recompensados a través de un mecanismo de pagos para aquellos más eficientes y rápidos en realizar los registros.

La lógica de trabajo es sencilla: Primero deberá instalar un programa en su computador conectado a internet. Todos los participantes que hayan instalado este software competirán para realizar los registros. La prueba que deberán pasar para confirmar una transacción será resolver un puzle matemático de encriptación de alta complejidad. Los primeros en resolverlo tendrán el privilegio de realizar el registro, y recibirán como pago unidades monetarias (nuevas) del mismo registro.

Sólo ganará el que más poder de cómputo tenga, dado que resolverá el puzle matemático en menos tiempo. ¿Registrar unidades ya no queda sólo en manos de un ente central (servidor) como un banco (unidades tales como los pesos) o una corredora de bolsa (unidades de valor como las acciones)? Así es, ese monopolio de registro queda ahora en manos del mercado (se les llama mineros), compitiendo por lograr presentar el nuevo estado del registro en el menor tiempo posible.

Al lograrlo alguno de los participantes, todo el resto de los mineros actualizan sus registros y se inicia una nueva competencia por el siguiente bloque de transacciones. En el protocolo de Bitcoin, esto sucede cada 10 minutos. En cada período de 10 minutos son creadas nuevas monedas y entregadas a las billeteras del minero que logró resolver el ejercicio matemático. Además, la parte interesada en realizar la transacción pagará una "pequeña" suma adicional por concepto de costos de transacción.

Las tarifas por transacción en la red de Bitcoin se determinan de manera dinámica, y dependen de cuánto es el tiempo máximo que el usuario está dispuesto a esperar por confirmar la transacción. Al momento de escribir este artículo, el tiempo medio de espera es de 25 minutos, y el costo de la misma es 9000 satoshis, lo que equivale aproximadamente a $1 USD. Si se considera que, a través de Bitcoin, se puede realizar una transferencia de valor a cualquier parte del mundo, este costo y tiempo son bastante bajos considerando que, por ejemplo, el costo de una transferencia para personas a través de la red internacional SWIFT es de aproximadamente $22 USD para montos de hasta $1000 USD, y que puede tardar desde varias horas hasta días en ser confirmada.

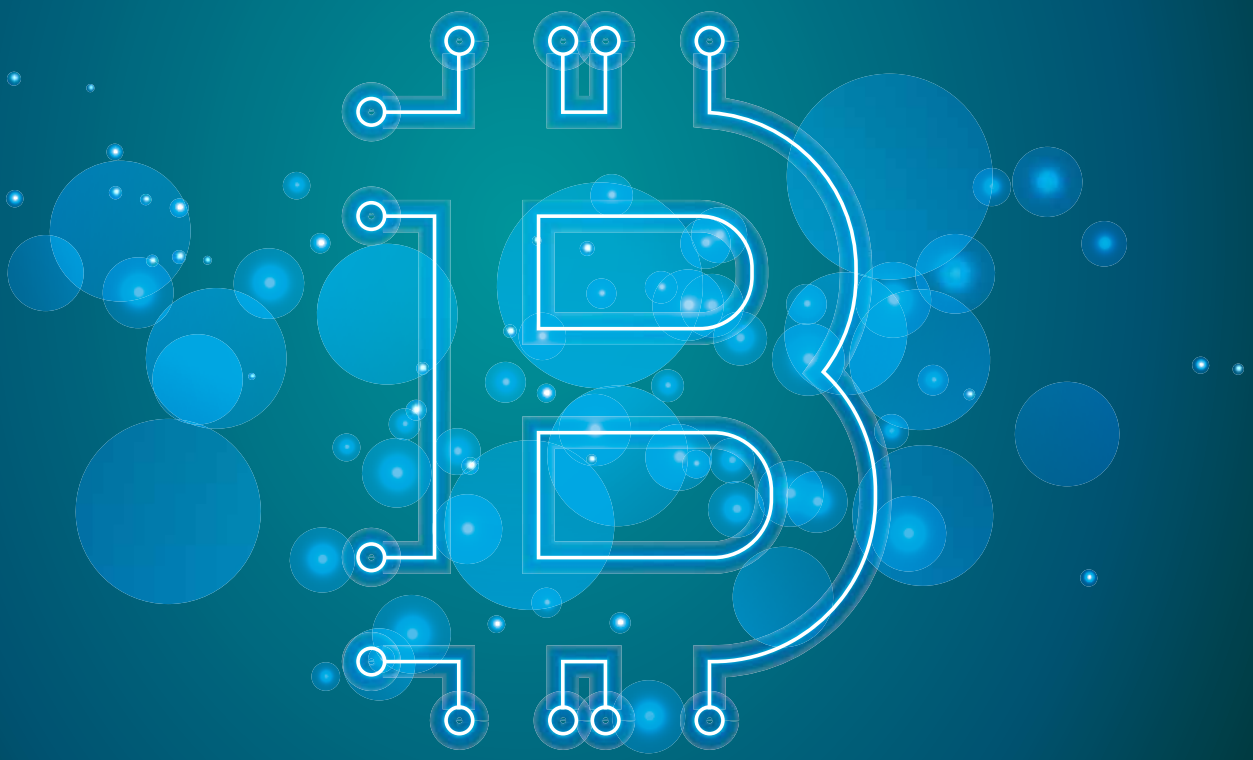
Satoshi Nakamoto imaginó y describió, además, un protocolo que permitiría evitar el mayor problema que existía hasta ese momento en el intercambio de unidades digitales: el doble gasto. En el mundo no virtual, cuando entregamos un billete o una moneda en forma de pago, hemos transferido sin lugar a duda la propiedad de ese billete o moneda. El problema que enfrentaban las tecnologías de transferencia de valor P2P (peer-to-peer) es que un archivo o registro digital puede copiarse un sinnúmero de veces a un costo casi cero.

El protocolo propuesto por Satoshi asegura que nadie pueda gastar las mismas unidades de valor dos veces: a medida que las transacciones se confirman, éstas van formando una cadena pública de registros que incluye tanto la información de la transacción realizada como las firmas digitales de las partes involucradas. Así, para ingresar un nuevo registro a esta cadena pública, las solicitudes de transacciones serán firmadas con llaves privadas encriptadas y confirmadas por una red descentralizada de computadores alrededor del mundo. A este registro público histórico inmutable, que asegura que no exista el doble gasto, se le llamó cadena de bloques o Blockchain.

## ¿Cómo funciona un Blockchain?:

Basado en principios criptográficos, este sistema permite prescindir de la confianza entre las partes involucradas, llevando un registro público seguro sin la necesidad de tener que confiar en un tercero central que lo confirme o lo consolide, y que no pueda ser revertido o alterado en el tiempo.

1 Aún se debate si Satoshi Nakamoto es una persona real, o un pseudónimo usado por el grupo de individuos detrás de la creación de la tecnología.



Cada dueño de una cuenta en el blockchain posee dos llaves, una pública y una privada. La pública es el equivalente a un número de cuenta bancario, el cual permite que un tercero pueda transferir unidades de valor a dicho registro. La llave privada es el equivalente a una clave segura, que será solicitada por el sistema cada vez que su dueño desee realizar una transacción.

El registro blockchain es construido como una cadena de firmas digitales, dado que cada dueño de una cuenta firma un hash [2] de la transacción previa con su llave privada, agregando a ese hash la dirección pública (billetera) del destinatario.

Dado que la firma (llave privada) se va registrando junto con la transacción y la marca de tiempo, no se considerará ninguna transacción más de esa cuenta en particular luego de firmar el hash. De este modo se forma una cadena que re-afirma el status quo del registro en un momento del tiempo.

Para ingresar un nuevo bloque de transacciones al registro, los mineros deben encontrar un número primo arbitrario asociado al bloque a ser registrado, que sólo puede ser usado una vez, denominado "nonce". El nonce, entonces, es un número primo único cuyo valor se establece de modo que el hash del bloque con ese nonce sea igual a una seguidilla de ceros.

Dado que es imposible predecir qué combinación de números se traducirá en el hash correcto, se deben probar iterativamente muchos nonce diferentes hasta encontrar el adecuado. Como esta búsqueda requiere tiempo y capacidad de cálculo computacional, mostrar a la red el nonce que resuelve el problema de encriptación constituye una prueba de trabajo. Una vez logrado el cálculo, cualquier modificación del registro, por mínima que sea, hará que el nonce ya no sea válido, por lo que, si una parte maliciosa quisiera alterar algún registro antiguo en la cadena, tendría que rehacer el trabajo computacional para encontrar cada uno de los nonces necesarios, lo que en teoría le podría tomar una cantidad de tiempo literalmente infinita.

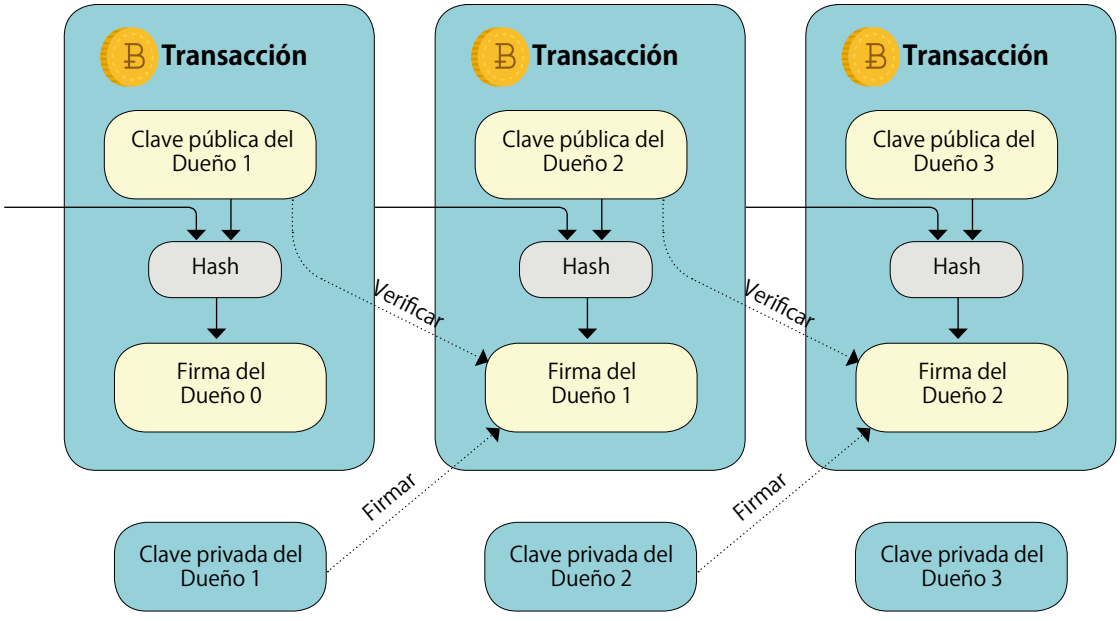
Como una segunda medida de seguridad, el protocolo de blockchain va requiriendo que el número de ceros del hash asociado al nonce sea cada vez mayor. En otras palabras, si la red está resolviendo los problemas demasiado rápido, la dificultad del cálculo aumenta.

## Más allá del Bitcoin: El valor de la tecnología subyacente blockchain

Podemos entender ahora que el nacimiento de Bitcoin trajo consigo la creación de una tecnología de registros segura y descentralizada; un registro público de unidades que cambia su estado bajo reglas que mezclan tiempo, matemática, encriptación y descentralización, con reglas de mercado. De este modo, los participantes que realizan transacciones y compiten por confirmar transacciones crean el valor de la unidad que se transa y registra en esa cadena de bloques. Más aún, democratiza los mercados financieros, bajando los costos de transacción, y permite el acceso universal: cualquier persona puede crear una cuenta en el Blockchain con un celular con internet.

Si bien el blockchain de Bitcoin fue el primero en operacionalizar esta lógica descentralizada, hoy existen nuevos protocolos que permiten incluso instalar aplicaciones computacionales dentro de ellos. Una de las nuevas redes más connotadas que permite la ejecución de los denominados "Smart Contracts" es conocida como Ethereum.

**Figura 1**




Tomada de Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System"

2 Recomendamos leer el apartado al final del artículo.

La gran diferencia con el blockchain de Bitcoin es que Ethereum permite a sus usuarios escribir un software que será "instalado" y ejecutado de manera descentralizada en su red. Por ejemplo, podríamos escribir una app de apuestas, en que el contrato inteligente consistiera en pagar automáticamente el pozo acumulado a todos los participantes que hayan acertado al resultado deportivo de interés.

Tanto el software como su data y los pagos asociados serán ejecutados y almacenados automáticamente en Ethereum, registrándose el estado más reciente de las aplicaciones instaladas en su red. Éstas van desde un procesador de texto u hoja de cálculo, hasta una página web, una casa de cambios virtual, un registro de inventario descentralizado, una bolsa de valores en la nube, etc. De manera similar al blockchain de Bitcoin, en la red Ethereum los mineros reciben un pago por almacenar y ejecutar los softwares, y compiten por ser los primeros en ejecutar las lógicas de los contratos inteligentes cada vez que sus usuarios lo requieran. Para realizar los pagos de los costos de ejecución sobre Ethereum, existe una moneda denominada ether, y es una de las criptomonedas que más capitalización ha captado en los últimos años.

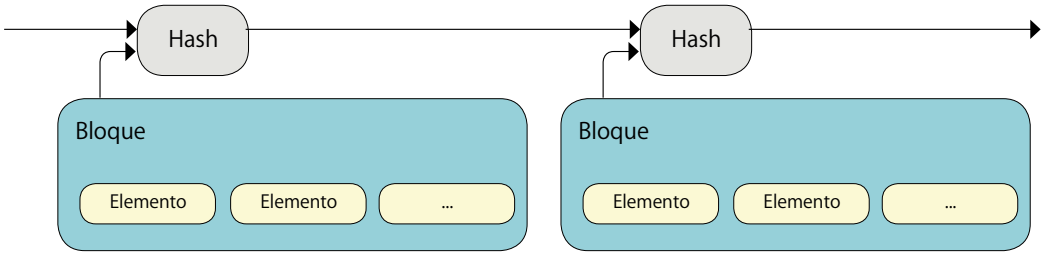
Dada la gran potencialidad de Ethereum, grandes empresas multinacionales, entre las que se incluyen BBVA, CISCO, Deloitte, ING, Pfizer, Santander y Scotiabank, se han unido para formar la Enterprise Ethereum Alliance, cuyo objetivo es explorar potenciales usos de dicha tecnología. Éstos van desde aplicaciones financieras, hasta de administración de la cadena suministros y proveedores, registro y autentificación de datos de salud, aplicaciones gubernamentales, mercados eléctricos, etc. Asimismo, otros actores ligados al mundo tecnológico, encabezados por Microsoft, han creado el consorcio R3, dedicado a crear un nuevo sistema operativo para mercados financieros basado en el concepto del libro mayor distribuido (distributed ledger), y han creado su propio blockchain denominado CORDA.

En Chile también hemos comenzado a ver la aparición de empresas locales, con iniciativas que van desde plataformas descentralizadas hasta servicios de pago. En el primer caso está Godzillion.io, una DApp desplegada como una arquitectura de contratos inteligentes en el blockchain de Ethereum. Opera con un token llamado GODZ, el que permite votar, invertir y transar porciones de propiedad de empresas start-ups, todo dentro del mismo blockchain. El segundo caso es CriptoPago.io, un servicio que permite a las personas y empresas cobrar en criptomonedas globalmente y recibir dinero fiat (pesos en este caso) localmente en sus cuentas, sin exponerse a la volatilidad de las monedas.

Por el momento, podemos concluir que Bitcoin, Ethereum, y otros blockchain y sus tecnologías subyacentes representan un nuevo paradigma en el registro e intercambio de información sin la necesidad de un ente central. ¿Cambiará la manera en que concebimos el mundo? Lo más probable es que sí, y mucho más velozmente de lo que esperamos.

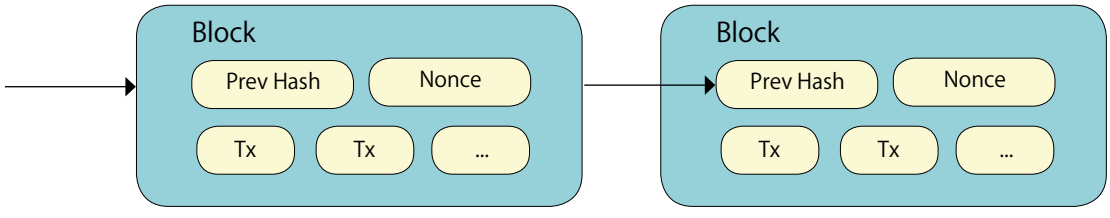


**Figura 2**




Tomada de Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System"

**Figura 3**




Tomada de Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System"

## Funciones Hash

En computación y criptografía, los hash o funciones de resumen son algoritmos que transforman una entrada o input (que puede ser una contraseña, un texto, o un archivo) en una combinación de caracteres alfa-numéricos con ciertas propiedades. Una de las principales características es que la combinación de caracteres resultantes es única y solo puede recrearse siguiendo las reglas de la función hash escogida y utilizando el mismo input. Así, podríamos entender una función hash como una operación computacional que permite crear una huella digital, teóricamente única, de una contraseña, texto o archivo. A la posibilidad de que la función hash pueda crear dos output o salidas iguales ante dos inputs distintos, propiedad claramente no deseada, se le denomina colisión. Una colisión entre hashes supondría la posibilidad de la existencia de dos documentos distintos con la misma huella digital.

Por ejemplo, una función hash muy sencilla (y muy poco segura porque no garantiza que no existan colisiones) podría establecer que cada vocal del input debe cambiarse por el número de posición en el alfabeto, y que las consonantes deben mantenerse igual que en la entrada. Asimismo, la función puede establecer que el hash resultante siempre debe tener 15 caracteres de longitud, y que, si el output tiene menos de 15 caracteres de largo, debe completarse el output con números correlativos. Así, el hash de aplicar nuestra función a la palabra "computador" será H(computador)=c16 MP2 2T1 D16 R12

Actualmente existen familias de funciones de hash que son reconocidas por minimizar las probabilidades de que existan colisiones de sus outputs. Dentro de las más conocidas se encuentran las SHA (Secure Hash Algorithm) publicadas por el Instituto de Normas y Tecnologías NIST de EE.UU. Incluyen las diferentes versiones SHA-1, SHA-2 (formada por diversas funciones: SHA-224, SHA-256, SHA-384, y SHA-512) y la más reciente, SHA-3. Las funciones hash SHA son inspiradas por el algoritmo MD2 y sus sucesores, creada originalmente por Ronald Rivest en 1989.

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | B | C | D | **E** | F | G | H | **I** | J | K | L | M | N | Ñ | **O** | P | Q | R | S |
| **1** | 2 | 3 | 4 | **5** | 6 | 7 | 8 | **9** | 10 | 11 | 12 | 13 | 14 | 15 | **16** | 17 | 18 | 19 | 20 |
| T | **U** | V | W | X | Y | Z | | | | | | | | | | | | | |
| 21 | **22** | 23 | 24 | 25 | 26 | 27 | | | | | | | | | | | | | |



Referencias:
Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System".
https://bitcoin.org/bitcoin.pdf
https://en.bitcoin.it/wiki/Protocol_documentation
https://coinmarketcap.com/currencies/bitcoin/
https://entethalliance.org/
https://www.r3.com

SOBRE LOS AUTORES

**David Díaz S., Ph.D.**
**Profesor Asistente, Departamento de Administración**
**Universidad de Chile**

**Cristóbal Pereira Garretón**
**Co-Fundador & COO**
**mifutu.ro**

**Rodrigo Sainz Palma**
**Co-Fundador & CEO**
**mifutu.ro**