Foto: Oscar Aldair Morales

Carlos Arcila, profesor de la Facultad de Administración y líder del Centro de Investigación de Mercados Financieros de Los Andes.

> “Una *digital fiat currency* es emitida y controlada por la autoridad monetaria del país y está sometida a las políticas estatales. No es un medio de pago supranacional”.

cada país y está sometida a las políticas estatales. “No es una moneda privada emitida por una empresa, ni es un medio de pago supranacional”. En su conferencia también explicó que desde 1970 el dinero no está respaldado por oro, por lo cual “el valor de una moneda depende de la aceptación y la confianza que la gente tiene hacia ella. Estas se expresan en tres características: sirve como medio de pago —se obtienen bienes a cambio—, es una medida de valor —por cuántas unidades se entrega un bien— y representa un depósito de valor, es decir, se puede ahorrar”.

Esa confianza se vio perjudicada durante la crisis financiera del 2008 y coincidió con la publicación del documento “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, de Satoshi Nakamoto (http://bit.ly/2nyo20g), un personaje cuya existencia no se ha demostrado, que dio origen al bitcóin y le permite al consumidor no depender de un sistema por entonces profundamente cuestionado.

Aunque el mundo financiero recuperó su credibilidad de la mano de los gobiernos que acudieron a su rescate, las criptomonedas han subsistido de manera alterna, sin otra regulación que la proporcionada por millones de usuarios y, por lo tanto, expuestas al riesgo. Según Carlos Arcila, la coexistencia de las *digital fiat currency* con el papel moneda y las digitales es tema de estudio en todo el mundo: “¿Cómo converge con el bitcóin y la moneda centralizada? Es una pregunta que todavía no está resuelta”.

Tampoco es clara la función, en este escenario, de la banca comercial, si sería sustituida por empresas de tecnología que se encargarían de verificar las transacciones y de gestionar las plataformas de *blockchain* sobre las cuales se montaría el sistema de la criptomoneda nacional. ■

ABC del bitcóin

Esta es la primera tecnología abiertamente inmutable. El programador que vaya a trabajar en la cadena de bloques necesita entender cómo funciona para hacerlo bien.

“De una manera genial que nadie había intentado antes, Satoshi Nakamoto diseñó bitcóin como un sistema de pagos basado en conceptos criptográficos conocidos desde 1980, pero combinados con gran ingenio”.

Así lo afirmó Milton Quiroga, criptógrafo de formación, en la conferencia “Las tecnologías detrás de bitcóin”, en la que habló de los principios técnicos que sustentan el bitcóin. Este ingeniero de sistemas uniandino es profesor de la Maestría de Seguridad de la Información del DISC y gerente fundador de la empresa CyberTech de Colombia. Nakamoto es el nombre con que se conoce al creador de bitcóin.

El profesor Quiroga dijo en su charla que la tecnología criptográfica tras la criptomoneda no es exclusiva del dinero digital, y como es genérica se puede aprovechar para acreditar la seguridad de todo tipo de registros digitales en los que la garantía de inmutabilidad sea muy importante.

Explicó que la *blockchain* de bitcóin trabaja de una manera específica que la hace muy segura, pues es descentralizada, es decir, miles de nodos distribuidos en el mundo efectúan las operaciones y verifican las transacciones. Además, es inmutable: cualquier modificación de un dígito en un bloque cambia todos los subsiguientes de la cadena, lo que lleva a que ningún dato se pueda borrar. La *blockchain* de bitcóin se construyó con código *open source*, bajo licencia del MIT, con la contribución de más de 400 programadores en todo el mundo.

En entrevista con revista Foros ISIS Milton Quiroga definió los principales elementos tras esta tecnología:

Bloque: Los de bitcóin están compuestos por los códigos de 2400 transacciones;

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84, 221. 736. 820. 214. 11. 60. 760.

Imagen de un bloque de blockchain.

Imagen: No machine-readable author provided. Historicair assumed (based on copyright claims). [GFDL (http://bit.ly/1fd019p), CC-BY-SA-3.0 (http://bit.ly/K9eh9h) or CC BY-SA 2.5-2.0-1.0 (http://bit.ly/2jcrgPn)], vía Wikimedia Commons.

hasta la fecha del foro se habían generado 495.804 bloques. En una *blockchain* privada se puede establecer un protocolo específico para que se cree un bloque cuando se cumplan ciertas condiciones.

De cualquier transacción en *blockchain* —la compra de un apartamento, una hipoteca, la escritura pública— no hay varias copias, sino una única a la que tienen acceso las partes involucradas en el negocio. Se le llama *ledger* o libro mayor.

Nodo: Cada grupo que mina —distribuidos por el mundo— en la plataforma de bitcóin conforma un nodo (en noviembre del 2017 eran 10.457) y trabaja con un *software* que transforma las transacciones a códigos. En una *blockchain* privada de bancos, por ejemplo, cada entidad sería un nodo de esa cadena.

***Hash*:** Es una función matemática para verificar alteraciones de un archivo. Para ello, hoy se emplea el algoritmo SHA256 o el llamado *scrypt*. La función de *hash* garantiza que si hay un cambio en el bloque 1000 y ya se han completado 10.000, habría que modificar los siguientes 9000. Cuantos más bloques se minen, más segura se hace la cadena y genera mayor confianza.

Minero: En bitcóin, su tarea es generar la confianza de la gente, pues es el encargado de encontrar el *nonce*. Pero en una *blockchain* privada y en cada caso habría que revisar qué papel cumpliría. Si, por ejemplo, es una cadena de bloques del Banco de la República, o de una empresa comercial con sus proveedores, esas entidades crearían los bloques. No se requerirían mineros privados, porque la información estaría centralizada en las máquinas de la organización.

Nonce: Es un número que constituye un desafío para los mineros: deben hallar un *nonce* tal que los resultados de *hash* tengan cierto número de ceros a la izquierda. La complejidad radica en que solo es posible descifrarlo a "fuerza bruta", es decir, haciendo combinaciones y combinaciones, empezando en 1 hasta los millones de valores del *nonce* necesarios hasta encontrarlo.

Dificultad de minado: En bitcóin la dificultad de cálculo aumenta cada cuatro años, aproximadamente. A la fecha del foro esta había cambiado cerca de 246 veces. En enero del 2018 se midió en 14 *exahashes* por segundo: toda la red de bitcóin procesa un trillón de *hashes* en un segundo para encontrar los *nonces* adecuados. Para solventar esta dificultad, continuamente se están creando máquinas y programas dedicados únicamente a minería de bitcóin, para que el proceso sea más eficiente en términos de tiempo y de consumo de energía.

Algoritmo de consenso: Se usa en la *blockchain* de bitcóin. Si dos nodos encuentran el *nonce* al mismo tiempo, el algoritmo, de manera justa, resuelve quién se queda con la recompensa. ■

Foto: Oscar Aldair Morales

Milton Quiroga

Árbol de Merkle

Es una estructura binaria que permite mezclar en un solo valor los *hashes* de todas las transacciones hasta llegar a una cifra resumen. Con esta se verifica que no hay alteraciones y, por lo tanto, que el bloque de bitcóin es válido.

"Para mostrar que la transacción K está en el bloque basta con mostrar un "Merkle *path*" de solo cuatro *hashes* de 32b (128 bits en total)", dijo Milton Quiroga.

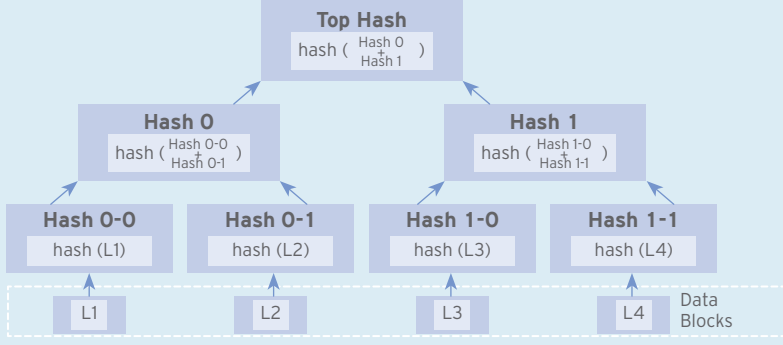

Imagen de Azaghal-Trabajo propio, CC0, https://bit.ly/2JsfBnO