DELTA PUBLICACIONES

CRIPTOMONEDAS

Relaciones con la economía, las finanzas, el marco regulatorio y la tecnología

Coordinador:
GUSTAVO TAPIA

Autores:
Ignacio Barbero
Sebastián Heredia
Daniel Miliá
Gustavo Tapia

CRIPTOMONEDAS

Relaciones con la economía, las finanzas, el marco regulatorio y la tecnología

CRIPTOMONEDAS

Relaciones con la economía, las finanzas, el marco regulatorio y la tecnología

Coordinador:
GUSTAVO TAPIA

Autores:
IGNACIO BARBERO
SEBASTIÁN HEREDIA
DANIEL MILIÁ
GUSTAVO TAPIA

DELTA
PUBLICACIONES

FICHA DE CATALOGACIÓN BIBLIOGRÁFICA

Título: Criptomonedas
Subtítulo: Relaciones con la economía, las finanzas, el marco regulatorio y la tecnología
Coordinador: Gustavo Tapia
Autores: Ignacio Barbero, Sebastián Heredia, Daniel Miliá y Gustavo Tapia
ISBN (libro impreso): 978-84-192-222-37
ISBN (libro digital): 978-84-19222-45-9
Edición: Primera
Año de edición: 2023
Páginas: 380
Formato: 17×24 cm
Área: Profesional, Universidad
Materia(s): KCBM - Economía monetaria
UDBM - Finanzas e inversiones en línea
GPJ - Teoría de la codificación y criptología
Encuadernación: Rústica

Editor gerente: Fernando M. García Tomé
Diseño de cubierta: Outdesign, Publishing Services
Preimpresión: Outdesign, Publishing Services
Impresión: Safekat

Reservados todos los derechos. De acuerdo con la legislación vigente podrán ser castigados con penas de multa y privación de libertad quienes reprodujeren o plagiaren, en todo o en parte, una obra literaria, artística o científica fijada en cualquier tipo de soporte sin la preceptiva autorización. Ninguna de las partes de esta publicación, incluido el diseño de cubierta, puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea electrónico, químico, mecánico, magneto-óptico, grabación, fotocopia o cualquier otro, sin la previa autorización escrita por parte de la editorial.

© 2022. Los autores
© 2023. Delta Publicaciones Universitarias, S.L.

Depósito Legal M-22766-2022
Impreso en España (UE) / Printed in Spain (EU)
(1122-15)

www.deltapublicaciones.com

Acerca de los autores

GUSTAVO TAPIA (Coordinador y autor)

Doctor por la Universidad de Buenos Aires (UBA) y Posdoctorado por UBA. Magister en Estrategia y Geopolítica (ESG). MBA por la UBA. Posgrado en Especialización Financiera en la Facultad de Ciencias Económicas (FCE) de la UBA. Contador Público por la UBA y docente de Grado, Posgrado y Doctorado en la UBA y otras universidades públicas y privadas. Coordinador de la Maestría de Finanzas y Profesor Titular Regular a cargo de cátedra de Administración Financiera en la FCE (UBA). Titular de cátedras de materias financieras en la Universidad de Belgrano. Investigador Categorizado-Director de Proyectos de Investigación UBACyT, Responsable del centro de investigación CEPAF y Consultor y Evaluador de Proyectos de Inversión. Responsable de la Agencia Calificadora de Riesgos Universidad Pública (UBA). Director de la Asistencia Integral para el Desarrollo Organizacional (AIDO). Autor de libros y artículos sobre finanzas y estrategia. Secretario del Instituto de Investigaciones en Gestión, Desarrollo y Control de las Organizaciones (IGEDECO) perteneciente a la UBA. Presidente de la Comisión Estudios sobre Mercado de Capitales y Finanzas de Empresas en el Consejo Profesional de Ciencias Económicas (CABA). Conferenciante nacional e internacional.

IGNACIO BARBERO (Autor del área tecnológica y sistemas aplicados a los negocios)

Ingeniero Industrial por la UBA. Experto en gestión de proyectos y reingeniería de procesos. Comunicador de Criptomonedas y protocolos descentralizados en Sector Público y Privado. Se desempeñó como responsable de tecnologías descentralizadas en la Aduana de Buenos Aires. Consultor técnico-comercial en diseño de tokens e ingeniería en Open Zeppelin.

DANIEL MILIÁ (Autor del área económico-financiera)

Licenciado y Doctor en Economía por la UBA, habiendo hecho una Maestría en Gestión Económica y Financiera de Riesgos y un Posgrado en Especialización Mercado de Capitales por la UBA. Además, ha cursado Posgrados en Docencia Universitaria por la UBA, siendo investigador en la UBA (CIMBAGE) y Universidad de Belgrano. Docente de 'Mercado de Capitales', 'Cálculo Financiero', 'Estadística I' en FCE UBA; de "Mercado de Capitales" y "Cálculo y Administración Financiera" en UB y en USAL. Autor de varios libros y artículos de finanzas y mercado de capitales. Conferenciante nacional e internacional.

SEBASTIÁN HEREDIA (Autor del área jurídica aplicada a los negocios)

Abogado (Universidad Católica de Córdoba). Magister en Derecho Empresario (Universidad Austral). Especialista en Corporate Finance (ESADE Business & Law School). Magister en Finanzas con orientación Fintech (ESADE Business & Law School). Egresado de la Blockchain Summer School (Utrecht University). Co-Coordinador del Grupo de Trabajo Legal Argentina de LACChain, la blockchain de BIDLab. Director de la Especialización en Blockchain de ADEN Business School. Co-Director de la Diplomatura en FinTech, GovTech, RegTech y LegalTech en UCC. Director de la Sala de Derecho y Tecnología del Colegio de Abogados de Córdoba. Autor del Manual *Open-source, Smart Contracts: Qué son, para qué sirven y para qué no servirán?* y de más de 60 publicaciones sobre temas de su especialidad. Es Co-Fundador y CEO de Tokenize-IT, una compañía LegalFinTech que ofrece servicios legales, de asesoramiento financiero y de desarrollo tecnológico para el diagnóstico, diseño, arquitectura y desarrollo de ecosistemas tokenizados y soluciones en blockchain. Conferenciante nacional e internacional.

Presentación

El mundo digital ha tenido grandes avances y fenómenos que han traído un cambio de paradigma en el mundo de los negocios y las inversiones afectando estructuras financieras con los consiguientes riesgos y rentabilidades. Esta transformación que atraviesa a empresas, instituciones y personas, va gestando nuevos procesos de descentralización y autonomía en los decisores.

El nombre de criptomonedas es la combinación entre criptografía y moneda. La criptografía utiliza la matemática avanzada para proporcionar mayor seguridad al sistema dotándolo así de más confiablidad. Concomitantemente, las crisis económicas han desnudado la vulnerabilidad de los sistemas bancarios con creciente aumento de desconfianza en las instituciones financieras como también el padecimiento de un menor poder adquisitivo de la población a causa de la pérdida de riqueza por desvalorización de los billetes y monedas de curso legal con que deben transar.

En los últimos años ha proliferado la emisión y el uso de las denominadas monedas virtuales, digitales o criptomonedas. Están presentes en todos los medios de comunicación, y en los últimos tiempos hemos sido testigos de las importantes subas y bajas en sus cotizaciones. También de los intentos regulatorios y de las prohibiciones de algunos países sobre las operatorias en el sistema de pagos que utilizan criptomonedas.

Nos preguntamos, ¿qué son los criptoactivos? ¿si tienen futuro? ¿Con qué ventajas cuentan? ¿Cuáles son los riesgos comerciales y financieros? ¿Por qué se los regula? ¿Qué rol protagónico tienen los mercados de capitales? ¿Cómo incide el desarrollo de las cripto en la vida diaria de las personas y las organizaciones? A lo largo de este trabajo procuraremos dar respuesta a estos interrogantes, yendo de menor a mayor y sin perder rigor académico.

El libro inicia con una introducción sobre el dinero digital bajo infraestructura blockchain y se conforma de tres partes específicas para tratar sobre los tópicos técnicos, económicos-financieros y jurídicos.

La Parte I denominada “Filosofía y tecnología de las Criptomonedas”, consta de tres capítulos, a saber, respectivamente, “Dinero y contexto”; “Efectivo electrónico y bitcoin”; e “Implicancias del bitcoin y surgimiento de las criptomonedas”.

La Parte II, “Economía y Finanzas”, explica en el capítulo primero el rol de las criptomonedas en el sistema financiero y en el capítulo segundo los actores del mercado cripto. El capítulo tercero aborda la emisión de criptomonedas y el cuarto desarrolla los fundamentos del trading y las estrategias de inversión.

Finalmente, la Parte III, “Legalidad y Regulaciones. Marco regulatorio de los tokens criptográficos y actores del ecosistema”, explica los principales jurídicos sobre criptoactivos y la regulación de ellos a nivel comunitario en los capítulos primero y segundo de esta parte, para finalizar con el capítulo tercero que trata del Central Bank Digital Currencies, recomendaciones del GAFI, exchanges y wallets.

Se presenta una obra integral y actual sobre el tratamiento de las criptomonedas bajo el título *CRIPTOMONEDAS. Relaciones con la economía, las finanzas, el marco regulatorio y la tecnología*.

Contenido

INTRODUCCIÓN

Bitcoin y criptomonedas. Dinero digital soportado en Blockchain

El Bitcoin es una criptomoneda. Es una moneda electrónica, un protocolo y un software. La conjunción de estos componentes permite la realización de transacciones casi instantáneas entre pares (*peer-to-peer* o P2P) y, por consiguiente, pagos en todo el mundo con unos bajos costos, o incluso nulos, de procesado de dichas transacciones.

El efecto de operar bajo tecnología *peer-to-peer* posibilita evitar depender de una autoridad monetaria central que se encargue de la emisión y el control de dinero y por lo tanto no es factible manipular el valor de las criptomonedas o crear inflación produciendo más moneda. La propia red es la que gestiona las transacciones y la emisión de Bitcoins, que se generan a través de la llamada minería, de forma controlada y descentralizada. La criptografía garantiza la seguridad de las transacciones. Por ejemplo, se puede controlar que sólo el dueño de las monedas pueda

Esta nueva manera de operar ha implicado un cambio de paradigma nutrido de una filosofía de mayor autonomía y control sobre las transacciones comerciales y financieras soportada en la arquitectura de creación y de utilización que tienen las criptomonedas.

Son los usuarios del sistema los que implícitamente toman estas decisiones globales en un verdadero sentido democrático.

En los siguientes dos ejemplos se exteriorizará esta filosofía:

1. Como recompensa por colaborar con la red, los usuarios reciben Bitcoins. Hasta aquí, puede parecer que los usuarios podrían engañar al sistema para aumentar su recompensa, pero, por construcción del sistema, la mayoría de los usuarios tendrán que validar posteriormente esa recompensa. Por lo tanto, si el usuario la aumentase subrepticiamente, esa acción sería rechazada por el resto.

2. Un usuario *A* hace un pago con una Bitcoin *b1* a otro usuario *B*. Para evitar que posteriormente *A* vuelva a utilizar *b1* para pagar a un tercer usuario *C*, en Bitcoin, las transacciones se hacen públicas. Por lo tanto, cuando el resto de la red detecte la segunda transacción, la rechazará, imposibilitando una reutilización de *b1* por parte del usuario *A*.

No obstante, en este caso no hay una equivalencia de *"un usuario = un voto"*, ya que el peso de cada usuario depende de la potencia de cómputo que éste dedica a la red. Así, la ecuación anterior en Bitcoin sería más bien *"x% de cómputo = x% de votos"*. Por lo tanto, siempre y cuando más de un 50% de la potencia de cómputo de la red sea controlada por usuarios honestos, la red seguirá la evolución que estos decidan. La idea puede contemplarse como una *"democracia ponderada"* en función de la implicación en el sistema.

Bajo estas premisas, se crea un escenario económico y social totalmente nuevo hasta su aparición. Esto es así porque, de adoptarse Bitcoin, o un sistema equivalente, los gobiernos y autoridades financieras no podrían controlar la evolución del dinero de una forma directa. Sí podrían influenciarla de forma indirecta legislando sobre ella, pero nunca controlar su comportamiento. No obstante, una moneda electrónica no tiene un carácter nacional, sino internacional. Por lo tanto, legislar sobre ella de manera efectiva tiene mayor complejidad.

En cuanto a los actores que intervienen en el sistema, se pueden distinguir dos tipos de participantes, que componen dos conjuntos no necesariamente disjuntos:

- Usuarios normales: son usuarios del sistema Bitcoin. Compran y pagan bienes y servicios utilizando Bitcoins, produciendo transacciones del sistema.
- Mineros: son usuarios especiales que dedican potencia de cómputo a validar nuevas transacciones, creando lo que se conoce como bloques de transacciones. Los cálculos que tienen que realizar son muy costosos por lo que se ven recompensados por ellos.

Adicionalmente, hay un tercer rol que normalmente se ignora: los desarrolladores. El medio principal de Bitcoin es, en definitiva, un software. Como tal, necesita un desarrollo y mantenimiento activos para lo cual es imprescindible un equipo de desarrolladores. Ello no pueden tomar decisiones en lugar del sistema, pese a su posición aparentemente central y especialmente influyente, Por ejemplo: los desarrolladores podrían decidir que la recompensa por encontrar un nuevo bloque pasase a ser de 50 a 100 Bitcoins, pero si a la mayoría de los usuarios (o más bien a los que proporcionan más

de la mitad de la potencia de cómputo) estuvieran en contra de esa decisión, podrían cambiar a otro cliente software de Bitcoin que mantuviese la recompensa que ellos consideran justa. En un caso extremo, cualquiera podría implementar su propio cliente siempre y cuando sea compatible con el protocolo. Así, el servicio de los desarrolladores es imprescindible, pero con una influencia limitada y desde luego mucho menor que en el común de las herramientas software.

Las principales funciones y ventajas de las criptomonedas bitcoin, en primera posición del mercado son las siguientes:

1. **Libertad para enviar y recibir pagos.** Se puede realizar transacciones de dinero desde cualquier lugar del mundo y en cualquier momento, solamente usando móvil o o la computadora. Así entonces, no hay restricciones de horarios o de fronteras. Esta ventaja es más estimada sobre todo en países donde existen restricciones para el libre intercambio de moneda.

2. **Menos riesgos en los pagos.** Las operaciones con Bitcoins son seguras, irreversibles, y nunca se mandan datos personales o privados de los usuarios. En un negocio de ventas online, sirve para impedir estafas de pedidos no recibidos o de devoluciones fraudulentas.

3. **Más seguridad y control.** Son los usuarios quienes tienen el control total sobre sus operaciones, por eso es imposible que alguien fuerce cargos no deseados, como sí podría ocurrir con una cuenta bancaria normal. Además, como los pagos en esta red se pueden hacer sin que estén asociados a la información personal, hay un alto nivel de protección contra el robo de identidad.

4. **Sistema neutral y transparente.** Toda la información de la red Bitcoin está a la vista de todos los usuarios ya que está disponible en el blockchain. Ninguna persona ni institución privada puede manipular el protocolo, ya que este está encriptado para que sea completamente seguro.

En principio Bitcoin tiene valor porque es útil como moneda. De por sí, tiene las cualidades básicas del dinero, es decir, portabilidad; durabilidad; escasez; divisibilidad; reconocibilidad y fungibilidad. Lo novedoso es que no está basado en propiedades físicas, como sí lo hacen el oro y la plata, ni confía en autoridades centrales, sino que se sustenta en propiedades matemáticas.

El valor de la criptomoneda se funda en que se trata de un bien escaso y no devaluable, con un proceso de creación a través de la denominada minería de bloques y hasta alcanzar el límite que en el caso del Bitcoin es de 21 mi-

llones. El proceso de minería requiere de una infraestructura con equipos sofisticados y una cantidad de energía apreciable Para minar un bitcoin por ejemplo se necesita 1.53 x 1016 Joules (equivalente a diez tormentas eléctricas), lo que significa un gran esfuerzo económico y ambiental aun cuando la energía producida en un porcentaje mayoritario sea renovable. La compensación que obtienen los mineros por este trabajo son dos incentivos: nuevos Bitcoins que se ponen en circulación y la comisión de las transacciones que irá variando de acuerdo con los *halvings*[1], y que refiere a la exacta reducción a la mitad de la cantidad de Bitcoin que se reciben por cada bloque minado. Cada cuatro años se lleva a cabo un *halving*, reduciéndose el ritmo de producción de Bitcons a la mitad cuando se lleva a cabo. Esto provoca que hace que se reduzca de notablemente la cantidad de Bitcoin que genera la red y que haya una limitación en la oferta.

Le suma valor a la criptomoneda, también el hecho de que este activo digital y financiero no puede ser congelado o incautado por algún Estado ó al menos requiere de un procedimiento especial.

La minería de Bitcoins es el proceso de invertir capacidad computacional para procesar transacciones, garantizar la seguridad de la red, y conseguir que todos los participantes estén sincronizados. Los mineros reciben un problema matemático basado en cálculos aleatorios, diferente cada aproximadamente 10 minutos y quien más rápido lo resuelve logra los incentivos mencionados. Cada transacción de Bitcoins se irá registrando en la "blockchain" como si fuera un gran libro contable, en el cual se validan las operaciones y se certifican los saldos de cada usuario. Todo este ecosistema se denomina la *granja de minería Bitcoin*.

Se comprende mejor entonces que para el funcionamiento consistente del sistema de transacciones se opere con una solución basada en redes entre pares (*peer-to-peer*), manteniendo registros de transacciones que no pueden ser alterados sin tener que realizar complicados cálculos matemáticos para recomponer todo el sistema.

Recapitulando, las fortalezas del sistema son:

- El programa de incentivos planteado en la implementación de Bitcoin supone, en forma de recompensas en monedas, una clave para el fomento de la participación de usuarios en la red, actuando como nodos que realizan los cálculos complejos que se requieren.
- La seguridad de Bitcoin es bastante alta puesto que se basa en primitivas criptográficas de seguridad demostrada. Además, su arquitectura

[1] *Halving* es un término anglosajón que ha sido acuñado por el sector de las criptomonedas y cuya traducción literal al español es *reducir a la mitad*.

evita fraudes como el doble gasto de saldo de los usuarios o la alteración indebida de su política de funcionamiento.

- La escalabilidad del sistema, por diseño e implementación, hace que su desempeño en el medio y largo plazo esté afianzado.
- Es un sistema transparente por naturaleza, ya que cualquiera puede comprobar el origen y destino de la moneda transada.

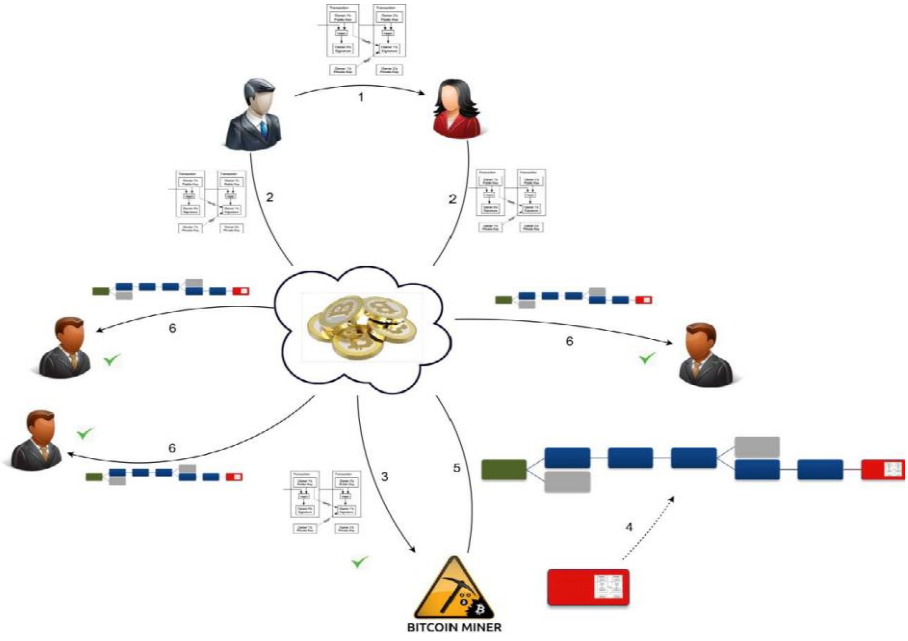
En cuanto a las debilidades mencionamos:

- Aunque segura por diseño, el funcionamiento de la red depende de otros elementos como los monederos dónde se almacenan las criptomonedas que selecciona el usuario requiriéndose de conocimientos de seguridad adicionales.
- Las comunicaciones entre los usuarios se realizan sin cifrar.
- Al tratarse de un sistema basado íntegramente en sistemas de información, su implementación está expuesta a posibles errores de programación y vulnerabilidades explotables por usuarios maliciosos para acceder al saldo de los usuarios.
- El hecho de que existan mecanismos independientes al sistema, mediante los cuales se puede reducir notablemente el anonimato de la red, junto con el hecho de ser un sistema transparente, puede suponer una grave amenaza para la privacidad de sus usuarios.
- La naturaleza de Bitcoin hace al sistema totalmente dependiente del consumo energético, necesario para realizar los cálculos complejos requeridos para su funcionamiento, lo que afectaría a los usuarios con costos más elevados

Conceptos y vocabulario ligado al mundo Cripto

- **Direcciones Bitcoin.** La dirección virtual de un usuario que contiene monedas Bitcoin y se utiliza para pagar y recibir cobros, similar a una cuenta de banco. Un mismo usuario puede tener tantas direcciones Bitcoin como necesite y se identifican con una clave pública. La dirección BTC es básicamente, una transcripción de una clave pública. La clave privada asociada sirve para firmar las transacciones y la clave pública sirve para identificar la dirección y validar las firmas.
- **Monederos.** Es un espacio virtual, equivalente a un monedero físico, donde se almacenan y gestionan direcciones Bitcoin de un usuario y los pagos que se realizan con ellas.

- **Transacciones.** Es una transferencia de dinero de una dirección Bitcoin *A* hacia otra dirección *B*. Para componer una transacción, el propietario de la dirección *A* firma una transcripción de la dirección *B* (entre otros datos) con la clave privada asociada a la dirección *A*, de forma que la red sabrá que el nuevo propietario legítimo es el dueño de la dirección *B*.
- **Bloques.** Es una estructura que agrupa transacciones. Las transacciones pendientes de confirmar se agrupan en un bloque sobre el que se realiza el denominado proceso de minería.
- **Cadena de bloques.** Registro público de las transacciones de BTC validadas en orden cronológico. Cuando un bloque ha sido confirmado, a través de la minería, éste pasa a formar parte de la cadena.
- **Minería.** Proceso de realización de cálculos matemáticos para confirmar transacciones en la red BTC. A través de la minería se pueden crear nuevas Bitcoins al mismo tiempo que se confirman transacciones.



– *B hace un pago en bitcoins a A.*
– *A y B envían la transacción a la red P2P de bitcoin.*
– *Un minero recibe la nueva transacción y la verifica.*
– *El minero crea un conjunto de transacciones nuevas, incluyendo la transacción del paso 1, y trabaja para confirmarla.*

- *El minero envía el nuevo bloque de transacciones confirmadas a la red P2P de Bitcoin.*
- *El resto de usuarios de bitcoin actualizan su estado incluyendo el nuevo bloque de transacciones, verificando que dicho bloque es válido.*

Conceptos criptográficos

Las primitivas criptográficas de las que bitcoin hace uso son las responsables últimas de que se consigan las propiedades de seguridad que se persiguen.

- **Firmas digitales.** Bitcoin utiliza el algoritmo ECDSA26 (Elliptic Curve Digital Signature Algorithm - Algoritmo de Firma Digital de Curva Elíptica) para firmar las transacciones, utilizando los parámetros recomendados por el Standards for Efficient Cryptography Group (SECG), secp256k1 [4]. Las firmas utilizan la codificación DER27para empaquetar sus componentes en un único flujo de bytes. ECDSA ofrece ventajas frente a otros esquemas de firma que lo hacen ideal para su utilización en un protocolo distribuido en Internet, como son: longitudes de clave y de firma muy cortas y generación y verificación de firmas muy rápidas.
- **Hashes criptográficos.** En los cálculos de hashes realizados en bitcoin se utilizan los estándares SHA-25628 y, cuando se requiere que el hash sea más corto, RIPEMD-16029. Normalmente el cálculo de hashes se realiza en dos fases: la primera con SHA-256 y la segunda, dependiendo de las necesidades de longitud del resultado, con SHA-256 o RIPEMD-160.

  Normalmente el cálculo de hashes se realiza en dos fases: la primera con SHA-256 y la segunda, dependiendo de las necesidades de longitud del resultado, con SHA-256 o RIPEMD-160.

  SHA-256(“Hola”) = E6 33 F4 FC 79 BA DE A1 DC 5D B9 70 CF 39 7C 82 48 BA C4 7C C3 AC F9 91 5B A6 0B 5D 76 B0 E8 8F

  SHA-256(SHA-256(“Hola”)) = A7 53 96 6A 11 02 90 57 D6 50 C4 C3 0C 2E 3F 52 8A B6 83 8B 96 C7 BA BB 74 3A EB 9E 3D 6B C4 01

  RIPEMD-160(SHA-256(“Hola”)) = F9 3B 68 56 C7 BD 9F 91 97 F7 B5 0F 35 93 09 EE 98 80 92 41
- **Números aleatorios y nonces.** Los números aleatorios y su generación son pilares fundamentales de la criptografía. Los *nonces* son números aleatorios “especiales” que, en principio, sólo se utilizan una vez (de ahí su nombre, que en inglés viene de ***n****umber used only once*),

aunque a veces los dos términos se utilizan de forma indistinguible. En Bitcoin, los números aleatorios y *nonces* se utilizan de forma directa para la generación de bloques. Como se verá a continuación, para obtener un nuevo bloque es necesario encontrar un número aleatorio que satisfaga ciertos requisitos. También se utilizan en Bitcoin, aunque de manera indirecta, como parte del algoritmo de firmas digitales (ECDSA).

- **Pruebas de trabajo.** Las pruebas de trabajo son el principal componente de Bitcoin responsable de garantizar que la red mantiene un comportamiento legítimo. Brevemente, esta idea hace que validar y calcular nuevos bloques de transacciones conlleve un costo computacional muy elevado, de forma que, para hacerse con el control de la red, un atacante necesitaría una potencia de cómputo extremadamente difícil de conseguir. El principal precursor de esta idea es el método Hashcash32. En concreto, en Bitcoin este control de complejidad en los cálculos para los nuevos bloques se realiza obligando a que el hash de cada nuevo bloque deba comenzar con un número determinado de ceros. Para el cálculo de este hash se combinan datos de bloques anteriores y un *nonce*. Dado que las funciones hash criptográficas no son invertibles, para encontrar un bloque válido la única alternativa será ir obteniendo diferentes *nonce* hasta encontrar uno que cumpla el requisito preestablecido.

PARTE 1

Filosofía y tecnología de las criptomonedas

IGNACIO BARBERO

ALGO DE HISTORIA Y EVOLUCIÓN

En algún punto entre 2009 y el presente fue posible por primera vez poseer y enviar dinero digital sin la necesidad de un intermediario que gobierne el sistema. No es posible precisar el momento puntual de este suceso. Podemos mencionar el 1º de noviembre de 2008, día en que Satoshi Nakamoto publicó el *whitepaper* de Bitcoin, como hito fundamental que habilita esta posibilidad. En este documento técnico de tan sólo ocho páginas describió concretamente el problema que intentaba resolver y una solución técnicamente viable para lograrlo. Pero no sería válido decir que Bitcoin era dinero allá por 2008.

De hecho, aún no existía una implementación práctica de lo propuesto teóricamente por Satoshi. Unos meses más tarde, el 9 de enero de 2009, se lanzó el primer cliente de software de código abierto para correr el protocolo de Bitcoin, y se registró la primera transacción. Hasta aquí, era sólo una prueba de software entre dos criptógrafos idealistas. El 5 de octubre de 2009, el sitio de compraventa de Bitcoin llamado *The new Liberty Standard* le puso precio a un Bitcoin por primera vez: 1309,03 BTC podían ser adquiridos por 1 dólar, un precio derivado de la cantidad de energía requerida para mantener el sistema en funcionamiento. El 22 de mayo de 2010, Lazlo Hanyecz ofreció 10.000 Bitcoins por dos pizzas en un foro de internet, concretando la primera transacción de Bitcoin por bienes o servicios y dando origen al "Bitcoin pizza day", un día icónico donde año a año la comunidad de Bitcoin celebra esta primera transacción.

No es posible precisar un hito que determine la constitución de bitcoin como dinero, ya que el dinero es un fenómeno social que requiere cierto grado de aceptación y consenso, que de no ser impuestos por decreto por el gobierno de turno, son cualidades se transmiten y se construyen gradualmente, con cada oferta y demanda individual del activo. Las propiedades únicas de Bitcoin sedujeron a miles de usuarios a invertir en esta moneda. Desde las primeras transacciones entre académicos y criptógrafos idealistas, pasando por entusiastas de la innovación, estudiosos del contexto geopolítico, osados inversores, curiosos, luego individuos que no deseaban quedarse afuera, empresas de diversos tamaños –pequeñas, grandes, multinacionales, y hasta Estados Nación.

La revolución tecnológica que propone la creación de Bitcoin no tiene impacto únicamente en el eje del dinero digital sin intermediarios. Los distintos componentes del protocolo que permiten esta funcionalidad abren un universo de posibilidades para el futuro de internet.

Este futuro con directrices claras pero enormes incertidumbres técnicas y sociales, ya ha sido conceptualizado como la "web3", una versión de internet donde

las bases de datos no están en control de un grupo relativamente pequeño de personas. La idea de web3 es más abstracta que la de sus predecesoras. La "web1" refiere al período entre los años noventa y los dos mil en que los sitios eran en su mayoría estáticos y los usuarios no podían interactuar con ellos ni generar contenido. La "web2" comprende el período posterior al dos mil -hasta el presente-, en el cual las grandes corporaciones de tecnología dominan el tráfico de internet habilitando generación de contenido por los usuarios y la interacción entre ellos. Este modelo demostró cómo los efectos de red tienden a converger el tráfico de internet en un puñado de corporaciones, que ofrecen servicios gratuitos a cambio de los datos personales de sus usuarios. Al aceptar sus términos y condiciones las principales aplicaciones que utilizamos diariamente guardan nuestra información personal: edad, sexo, lugares visitados, vínculos sociales, empleador y el nombre de nuestra mascota.[1] Pero la información recolectada por las grandes compañías va más allá: toda interacción que tenemos al navegar por internet es almacenada y procesada, revelando gustos, tendencias, patrones de consumos y una infinidad de información con gran valor económico.

En el año 2015, se estima que Facebook recolectaba diariamente 500 terabytes de datos, mientras que Google y Amazon tenían almacenados más de 10 y 1 exabyte (1000 terabytes) respectivamente[2]. Hacia 2021 la cantidad total almacenada de datos generados por usuarios de internet en el mundo era de 79 zettabytes (79.000.000.000.000 GB) y se prevé que sea de 175 ZB en el 2025[3]. Estas bases de datos representan un enorme poder que puede influir notablemente en la vida de las personas. La premisa de web3 es ofrecer y extender las bondades de sus predecesoras, permitiendo que usuarios no sólo publiquen contenido, sino que sean dueños del contenido, y que tengan voz y voto en los sistemas que gobiernan cómo esa información se transmite en la red.

Antes de Bitcoin, no era posible concebir un bien digital escaso y transable a través de internet sin una entidad responsable de llevar el registro de esa propiedad y de todas las transacciones ocurriendo en la red. La centralización de la administración de este registro trae consigo algunas cualidades indeseables en un sistema de transferencia de valor, que derivan principalmente de dos características intrínsecas de la centralización:

- Único punto de falla - Los servidores que guardan la información deben ser protegidos ante fallas del sistema eléctrico, accidentes y desastres na-

[1] Clario.Co. 2022. *Big brother brands report: which companies might access our personal data the most?* [online] Available at: <https://clario.co/blog/which-company-uses-most-data/> [Accessed 19 February 2022].

[2] PRICE, D. (2015, March 17). *Infographic: How much data is produced every day?* CloudTweaks. https://cloudtweaks.com/2015/03/how-much-data-is-produced-every-day/

[3] REINSEL, D., GANTZ, J., y RYDNING, J. (2018).

turales. Asimismo, deben proteger los sistemas de hackers externos, así como de estafas del personal interno con acceso privilegiado.

- Neutralidad de la red - El administrador tiene control sobre lo que sucede en el sistema. Puede alterar el contenido de la base de datos, censurar usuarios o transacciones a su conveniencia, y extraer valor de la información de los usuarios.

El impedimento para construir un sistema descentralizado y robusto para transferir dinero ha sido principalmente uno técnico, formalmente conocido como el "Problema del doble gasto". Este problema es propio de los esquemas de monedas digitales (efectivo digital) y es particularmente difícil de resolver para sistemas descentralizados. Más de 100 esquemas de efectivo digital fueron propuestos durante los años 90' y los 2000'[4], algunos de ellos efectivamente implementados, pero todos con fallas fatales que impidieron su adopción masiva. La solución llegó con el *paper* de Satoshi Nakamoto en 2008, y demostró ser suficientemente robusto para permanecer en funcionamiento por al menos 13 años, con una masiva base de usuarios incluyendo fundamentalistas y predicadores de las bondades de esta moneda digital.

Las criptomonedas son el resultado de desarrollos tecnológicos en criptografía y redes, y la voluntad de los participantes de estos protocolos para utilizarlos. Pero la motivación para concebirlos tiene un fuerte componente político, y una ineludible conexión con una ideología económica. La forma en que estas áreas de conocimiento se interrelacionan para dar a luz a Bitcoin es apasionante y merece ser analizada de forma holística. Quienes se embarcan en la tarea de comprender la relevancia de Bitcoin coinciden que se trata de un 'agujero de conejo', refiriéndose a la profundidad de conocimiento en diversas áreas a las que uno puede acceder en la búsqueda de respuestas, todas revelando componentes interesantes de la historia y la actualidad, generando preguntas sobre los sistemas que elegimos para coordinarnos como sociedad y sobre sus orígenes, sobre los orígenes del dinero y su significancia más fundamental, y eventualmente sobre conceptos abstractos que podrían ser adecuados para su estudio en academias de filosofía, como son la libertad y la privacidad, pero que tienen implicancias prácticas con ejemplos visibles en nuestra vida cotidiana, y cuyos efectos son amplificados por la masiva explosión de transacciones que posibilita la internet.

[4] BONNEAU J, FELTEN E, MILLER A, y GOLDFEDER S. (2016).