DOCENTES DE ADMINISTRACIÓN FINANCIERA

42 Jornadas Nacionales de Administración Financiera
Septiembre 22 y 23, 2022

Dinero digital

Bitcoin y cripo en infra-estructura *blockchain*

Gustavo Tapia
Ignacio Barbero
Daniel Miliá
Universidad de Buenos Aires – Universidad de Belgrano

SUMARIO

Para comentarios:
gustavo.tapia1@gmail.com
daniel@economicas.uba.ar

1. 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. Es difícil precisar un momento puntual a partir del cual esta posibilidad se convirtió en una realidad. 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 8 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, en 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 compra-venta 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.

El dinero es un fenómeno social que requiere de alguna aceptación y consenso, a excepción de las imposiciones de gobiernos. El dinero y como observamos en este proceso, también el bitcoin posee cualidades que se transmiten 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 por individuos que no deseaban quedarse afuera de esta transformación −aunque no entendieran muy bien la tecnología y la implicancia de sus cualidades únicas−, 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 aó 2000 (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 hasta el 79,49% de 45 ítems posibles de información personal, desde

edad y sexo a lugares visitados, vínculos sociales, empleador o nombre de mascota. 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 2015 se estimaba que Facebook recolectaba diariamente 500 terabytes de datos, mientras que Google y Amazon tenían almacenados más de 10 y 1 exabyte (1000 terabytes) respectivamente. Hacia 2021 la cantidad total almacenada de datos generados por usuarios de internet en el mundo era de 79 zettabytes (40.000.000.000.000 GB) y se prevé que sea de 175 ZB en 2025. 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 los 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 naturales. 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 1990 y 2000, 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 robusta 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 significado

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.

Las preguntas que surgen son: ¿Por qué es tan importante evitar la centralización en el dinero digital? ¿Qué motivación perseguían los académicos y criptógrafos que emprendieron esta búsqueda? Responder estas preguntas requiere profundizar en la naturaleza y la historia del dinero, la evolución de los sistemas de organización social, y en particular, una serie de eventos que sucedieron en los Estados Unidos tras el final de la segunda guerra mundial.

2. Funciones. Ventajas y desventajas

El bitcoin es una criptomoneda y, como 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 costo bajo, o incluso nulo, de procesado de dichas transacciones.

El efecto de operar bajo tecnología *peer-to-peer* evita la dependencia 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. 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. Así, 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. 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 de 50 a 100 bitcoins, pero si 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 criptomoneda 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 la computadora. 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 dada su disponibilidad 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 millones.

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 a 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 se reduzca 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 o 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 diez minutos y quien más rápido lo resuelva 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 evita fraudes como el doble gasto de saldo de los usuarios o la alteración indebida de su política de funcionamiento.

[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*.

- 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.

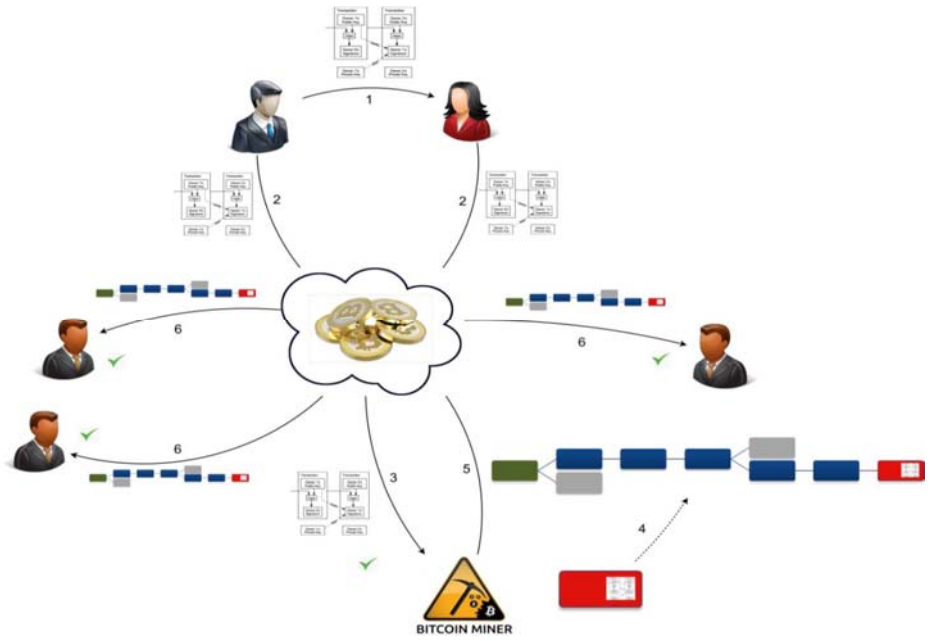
En cuanto a las debilidades mencionaremos:

- 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

3. 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.

4. 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.

5. Consideraciones finales: Bitcoin como *el nuevo dinero*

Bitcoin nació como un experimento de monetizar la tecnología en internet, concebido en plena crisis subprime en 2008, y es una verdadera innovación que generó un cambio sin precedentes para la humanidad, ya que se transitó de un sistema de dinero que rigió durante siglos, a una forma más coherente a nuestra época, creado y alojado por el internet.

Es hasta ahora, el dinero más complejo que se haya creado, aunque también el más perfecto en términos de eficiencia. Podemos argumentar eso ya que ha resuelto, a través de algoritmos, los grandes problemas que han presentado las distintas clases de dinero conocidas hasta ahora.

Pensemos solamente que una vez que el trueque se hizo insostenible debido a las dificultades naturales que presentaba el intercambio directo, principalmente inconvenientes de doble coincidencia (tanto en necesidad, como en sentido de escala y temporalidad) como de altos costos transaccionales (y por ende costos de oportunidad, medidos principalmente en tiempo gastado en buscar la coincidencia), la humanidad debió encontrar una solución a este problema, mediante algo que permita el intercambio indirecto, posibilitando la transferencia y almacenamiento de valor, creándose los primeros vestigios de dinero.

Como hemos referido, a lo largo de la historia, se han observado miles de ejemplos de dinero, expresados desde piedras gigantes e inamovibles en la isla de Yap −hoy Micronesia− como conchas marinas, sal, metales preciosos (oro y plata principalmente) llegando a las hoy ya conocidas monedas y billetes de curso legal expedidas −y reguladas sobre todo−, por los gobiernos a través de sus Bancos Centrales, también conocidas como monedas fiat.

Las criptomonedas han ofrecido mejoras a la solución de estos problemas, al perfeccionar las características clásicas del dinero fiat (y sus antecesores):

Como medio de intercambio (o medio de pago)

Para que un instrumento sea dotado de tal función debe ser ampliamente aceptado, siendo la característica esencial y por ende más importante que debe contener el dinero. Un medio de intercambio eficaz debe tener la facilidad de venderse como un producto (en este caso la moneda en sí misma) en el mercado, con el menor de los perjuicios sobre su valor.

Si bien los más agnósticos podrían sugerir que BTC no es un buen medio de pago, podemos argumentar que esa afirmación es cada vez más falsa, ya que a medida que su popularidad ha escalado, se han creado multiplicidad de mercados satélites donde operarlo, desde *exchanges* donde poder comprar y vender BTC -o la criptomoneda que se desee-, como así también plataformas que permiten adquirir productos o servicios nominados en cripto. Se observa que mientras más entusiastas se suben al tren de la cripto euforia, más amplio será el uso como medio de intercambio, ya sea de Bitcoin o de cualquiera de sus alternativas surgidas a lo largo del tiempo, las cuales mejoran determinadas características como disminuir la volatilidad de precios o aquellas que realizan pagos más veloces.

Como unidad de cuenta

Así como expresamos la distancia en kilómetros y sus subunidades fraccionarias, como los centímetros, el valor de los bienes y servicios se expresa en unidades monetarias y fracciones de éstas. Bitcoin, al igual que cualquier otra moneda tiene la propiedad de divisibilidad, pero exponenciada, ya que puede subdividirse hasta en 100 millones de unidades mínimas. Estas

fracciones mínimas de Bitcoin fueron bautizadas como Satoshis por la comunidad cripto (en honor a su creador, Satoshi Nakamoto). Otras criptomonedas de valor más estable, llamadas Stablecoins como ser el Tether, cuyo valor tiene paridad con el Dólar, siendo 1 Tether = 1 USD, también puede subdividirse en mayor cantidad de veces que un dólar tradicional, gracias a su naturaleza digital.

Como reserva de valor

Sobre esta propiedad del dinero, podemos entender su relevancia si pensamos en el trueque de antaño, cuando por ejemplo un productor agropecuario no podía almacenar su riqueza sin perder su valor debido a la descomposición natural de su insumo. Por ende, la resistencia y durabilidad de una moneda en cuanto a sus propiedades físicas es clave, pero también la fortaleza de su valor frente a la pérdida de valor adquisitivo en el tiempo. Se puede calcular dicha fortaleza con un simple cociente resultante de dividir su stock (existencia actual o circulante) en su flujo de nueva creación. Mientras mayor sea el resultado de dicho cociente, mayor fortaleza tendrá una moneda, ya sea que estemos hablando de piedras, conchas de mar, monedas fiat o el mismo bitcoin.

Esta cuestión se entiende mejor cuando analizamos las monedas de países devaluados y con hiperinflación, como podría ser la Alemania de posguerra o la Venezuela actual, cuyo aumento del flujo por emisión monetaria disminuye el ratio stock/flujo, con una consecuente disminución del valor de la moneda, presentándose como una pésima alternativa de ahorro en el largo plazo. Este problema, subsanado en bitcoin desde su código de programación, ha sido la piedra fundacional sobre la que se ha erigido, ya que la velocidad de creación de nuevos bitcoins disminuye en el tiempo por lo que su existencia será limitada Este comportamiento deflacionario que posee BTC, se encuentra en contraposición de las políticas monetarias inflacionarias que rigen las monedas fiat.

REFERENCIAS

Androulaki, E., Karame, G., Roeschlin, M., Scherer, T. & Capkun, S. (2013). *Evaluating user privacy in bitcoin*. International Conference on Financial Cryptography and Data Security FC 2013: Financial Cryptography and Data Security, 34-51

Certicom Research (2010). *SEC 2: Recommended elliptic curve domain parameters*.

Chaum, D. (1985). *Security without identification: Transaction systems to make big brother obsolete*. Communications of the ACM, 28 (10): 1030-1044

Chaum, D. (1981). *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM, 24 (2): 84-88

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. & Savage, S. (2016). *A fistful of bitcoins: Characterizing payments among men with no names*. Communications of the ACM, 59 (4): 86-93

Möser, M. (2013). *Anonymity of bitcoin transactions: An analysis of mixing services*. Münster Bitcoin Conference, July, 1-10

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Disponible en sitio web bitcoin.org

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A comprehensive introduction*. Princeton University Press

Price, D. (2015). *Infographic: How much data is produced every day?* CloudTweaks. https://cloud tweaks.com/2015/03/how-much-data-is-produced-every-day/

Reid, F. & Harrigan, M. (2011). *An analysis of anonymity in the bitcoin system*. 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, 1318-1326

Reinsel, D., Gantz, J. & Rydning, J. (2018). *The digitization of the World: From edge to core*. IDC White Paper

Ron, D. & Shamir, A. (2014). *How did dread pirate Roberts acquire and protect his bitcoin wealth?* International Conference on Financial Cryptography and Data Security, 1-11