

Bitcoin, la otra cara de la moneda

SOFÍA E. MANTILLA

Directora del Observatorio TICs del Instituto de Estrategia Internacional (IEI) de la CERA.

Editora del newsletter En Cont@cto Hoy.

Magister en Historia (UTDT), Lic. en Economía (UCEMA).

Este artículo explora el complejo fenómeno de Bitcoin, la criptomoneda creada a fines de 2008 que saltó a la fama mundial en 2013. En primer lugar, se analiza su origen y funcionamiento, y se describen los mecanismos que le imprimen sus particulares características. En segundo lugar, se profundiza en las diversas definiciones e interpretaciones que se han realizado en torno a Bitcoin, considerándose como dinero, activo, esquema Ponzi, protocolo y circuito alternativo para eludir a gobiernos y otras instituciones oficiales. En tercer lugar, se presentan dos desafíos que enfrenta para su crecimiento: la regulación gubernamental y la competencia de otras criptomonedas. Se concluye que Bitcoin logrará trascender ya que su tecnología subyacente, el Blockchain o cadena de bloques, tiene un potencial transformador de primera magnitud.

I. INTRODUCCIÓN

BITCOIN¹ ES MUCHAS COSAS A LA VEZ: UN protocolo de código abierto (*open-source*), una red descentralizada P2P (*Peer-to-Peer*), una criptomoneda², un sistema de pagos electrónico, y la solución de uno de los grandes problemas en la historia de la criptografía, el Problema de los Generales Bizantinos. Ha sido caracterizado de diversas maneras: una moneda, un activo, una *commodity* y un servicio operativo de pagos.

A nivel fundamental, *Bitcoin* permite la transferencia de valor, en forma de unidades digitales llamados *bitcoins*, de cualquier punto de la Tierra a cualquier otro –siempre que se tenga conexión a Internet– sin revelar la identidad del emisor o receptor. Los *bitcoins* tienen una existencia puramente virtual, no tienen entidad física ni correspondencia en el mundo real. No son emitidos por ningún Banco Central o institución, sino que son creados en un proceso llamado *minería* a un ritmo fijado en el protocolo mismo. Sumado a eso, el sistema está diseñado de modo tal que tampoco se requiere de un intermediario o tercero de confianza para verificar las transacciones. Barren con esta necesidad el poder de la criptografía y el consenso de una red descentralizada de *mineros* que operan con el *Proof-of-Work* (prueba de trabajo). Todas las operacio-

[1] *Bitcoin* con mayúscula se refiere al concepto y al protocolo, y *bitcoin* con minúscula a las unidades.

[2] *Cryptocurrency*, en Investopedia. Acceso online: <http://www.investopedia.com/terms/c/cryptocurrency.asp>

nes quedan registradas en el *Blockchain*, o cadena de bloques, un libro contable público, descentralizado e inalterable. En la actualidad, *Bitcoin* es más rápido y barato que los sistemas de pagos tradicionales y su tecnología subyacente tiene el potencial de servir como base para los contratos inteligentes y la transmisión digital de valor.

Bitcoin fue creado por Satoshi Nakamoto, pseudónimo de una persona o grupo cuya identidad aún es desconocida. El *whitepaper*, *Bitcoin: A Peer-to-Peer Electronic Cash System*³, fue publicado a fin de 2008 y la primera transacción se realizó a principios de 2009 a un precio nulo. En pocos años, la criptomoneda pasó de los márgenes de la afición tecnológica a las primeras planas de todos los diarios, cuando su valor superó los USD 1.000 en noviembre de 2013 y cuando Mt Gox, uno de los sitios de intercambio de *Bitcoin* más importantes del mundo, colapsó en febrero de 2014. Al 31 de enero de 2015, un *bitcoin* valía unos USD 230 y su capitalización de mercado era de alrededor de USD 3 mil millones⁴.

Desde sus inicios, *Bitcoin* se ha revelado como *locus* de disputas materiales y simbólicas. Para algunos, es una innovación revolucionaria en línea con la computadora personal e Internet, capaz de transformar procesos políticos (elecciones), industrias y actividades (bancarias, financieras), estructuras (corporaciones, sistemas de intermediación legal-burocráticas) y conceptos (confianza, propiedad, responsabilidad jurídica). Para otros, es una burbuja especulativa –la Tulipomanía de la Era Digital–, un esquema Ponzi o un caldo de cultivo para actividades sospechosas: lavado de dinero, financiamiento de actividades ilegales (terrorismo, trata), intercambio de bienes y servicios ilegales (drogas, armas, juego, pornografía infantil). *Bitcoin* ha sido considerado la materialización de una utopía libertaria y un pasatiempo alocado de los tecnólogos

de Silicon Valley, la solución para destronar al dólar estadounidense y una moda destinada a perecer. El hecho es que fue una inquietante novedad en las pos-trimerías de la Crisis Financiera Global de 2008-09 cuando se reavivaban los debates sobre la arquitectura de los sistemas financieros, el papel del dólar y la Reserva Federal y la relación entre los Estados, los individuos y el dinero.

En este informe se explorarán, en la Sección *Cimientos y arquitectura*, los cimientos sobre los cuales se construyó *Bitcoin*, y cómo su arquitectura le imprime sus particulares características. En *Interpretaciones de Bitcoin*, se profundizará en las diversas definiciones que se han dado de la criptomoneda. Se verá si cumple los requisitos necesarios para ser considerado dinero y las consecuencias económicas de su armado. Luego, se considerará como activo, se verá si es o no un esquema Ponzi, y se examinará como circuito alternativo para eludir a gobiernos y otras instituciones oficiales. También se indagará en su potencial transformador en tanto protocolo. La sección *¿Muerte e impuestos?* presentará dos desafíos con los que se ha topado *Bitcoin*: las reacciones de los gobiernos y la competencia de otras criptomonedas.

[3] NAKAMOTO, SATOSHI. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Acceso online: <https://bitcoin.org/bitcoin.pdf>

[4] Ver: <https://blockchain.info/> Datos del 31 de enero de 2015.

2. CIMIENTOS Y ARQUITECTURA

2.1 Los cimientos Cypherpunk

La idea de crear una moneda virtual no nació con *Bitcoin*. Su semillero fue el movimiento *Cypherpunk* que se formó a fines de los ochenta en EEUU. Sus integrantes –programadores, ingenieros, investigadores, entusiastas de la tecnología y pensadores de fuerte base libertaria– buscaban aplicar los principios de la criptografía para proteger la privacidad de los individuos frente a los Estados. Los fundadores más destacados son:

Eric Hughes: matemático de la Universidad de California Berkeley y autor de *A Cypherpunk's Manifesto* (1993). En este texto decía: *“La privacidad no es el secreto. Un asunto privado es algo que uno no quiere que todo el mundo se entere, un asunto secreto es algo que uno no quiere que nadie se entere. La privacidad es el poder de revelarse selectivamente ante el mundo [...] Por lo tanto, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimas”*⁵.

Tim May: físico, ingeniero, científico de Intel. Fue autor de *A Crypto Anarchist Manifesto* (1992) en el que vaticinaba: *“Así como la tecnología de la imprenta cambió y redujo el poder de los gremios medievales y la estructura de poder en la sociedad, los métodos criptográficos alterarán fundamentalmente la naturaleza de las corporaciones y de la interferencia del gobierno en las transacciones económicas”*⁶.

John Gilmore: programador de Sun Microsystems y fundador del Electronic Frontier Foundation. Abogaba por una *verdadera privacidad financiera* y creía que sólo la física y la matemática serían capaces de garantizar una *verdadera privacidad en las comunicaciones personales*⁷.

A fin de 1992, se creó *alt.cypherpunks*, una lista de emails encriptados en la que se realizaban intercambios de opiniones sobre tecnología, criptografía, privacidad, derechos civiles, política, comunicaciones y las intersecciones entre todas estas áreas. Entre los suscriptores más conocidos se encuentran Julian Assange, funda-

dor de Wikileaks; Bram Cohen, creador de Bit Torrent; John Young de Cryptome.org; Adam Back, creador del sistema de prueba de trabajo Hashcash; y Hal Finney, creador de la prueba de trabajo reutilizable y destinatario de la primera operación de *Bitcoin*⁸.

Una idea que despertaba especial entusiasmo en el grupo era la posibilidad de crear una moneda virtual que no dependiera de ningún gobierno para funcionar. Había un antecedente interesante. A principios de los ochenta, el doctor en sistemas David Chaum –*padre espiritual* de *Cypherpunk*– había presentado trabajos que sentaban las bases de una moneda digital y en 1990 había fundado DigiCash, una empresa de dinero electrónico basada en protocolos criptográficos (quebró en 1998 y Chaum fundó otra empresa llamada Ecash)⁹. Entre los *cypherpunks*, los debates e investigaciones cobraron cada vez más vigor. De ese clima intelectual emanaron diversas propuestas y experiencias, tales como E-gold (Douglas Jackson y Barry K. Downey), bitgold (Nick Szabo), RPOW (Hal Finney) y B-money (Wei Dai). Ninguna logró establecerse de modo sustentable, y algunas sólo fueron propuestas teóricas, pero las lecciones aprendidas a raíz de sus fracasos fueron clave como cimiento para el desarrollo de *Bitcoin*.

[5] HUGHES, ERIC. *A Cypherpunk's Manifesto*, marzo de 1993. Acceso online: <http://www.activism.net/cypherpunk/manifesto.html>

[6] MAY, TIM. *A Crypto Anarchist Manifesto*, noviembre de 1992. Acceso online: <http://www.activism.net/cypherpunk/crypto-anarchy.html>

[7] GILMORE, JOHN. *Privacy, Technology, and the Open Society*, 28 de marzo de 1991. Acceso online: <http://www.toad.com/gnu/cfp.talk.txt>

[8] BAROK, DUSAN. *Bitcoin: censorship-resistant currency and domain name system to the people*. Acceso online: http://www.academia.edu/771909/Bitcoin_censorship-resistant_currency_and_domain_name_system_to_the_people

[10] Ver, por ejemplo: CHAUM, DAVID. *Blind Signatures for Untraceable Payments*. Acceso online: <http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>; CHAUM, DAVID. *Security without Identification*. Acceso online: http://www.chaum.com/articles/Security_Without_Identification.htm

2.2 Satoshi Nakamoto, el misterioso arquitecto

Las discusiones sobre las monedas virtuales se fueron aquietando hasta que, a fines de 2008, apareció un trabajo que cambiaría para siempre el curso de los acontecimientos. Era *Bitcoin: A Peer-to-Peer Electronic Cash System*, el *whitepaper* de Bitcoin. El autor era Satoshi Nakamoto. Nadie había oído hablar de él. Su perfil *online* decía que vivía en Japón y su dirección de email correspondía a un servicio gratuito en Alemania. Nadie lo conocía. Las búsquedas de Google resultaban infructuosas. Evidentemente, se trataba de un pseudónimo¹⁰. Hasta el día de hoy su verdadera identidad es fuente de numerosas especulaciones. Algunos dicen que es Nick Szabo, algunos Wei Dai, algunos Hal Finney, otros creen que es una combinación de los tres, y otros aseguran que no es ninguno de ellos¹¹. En marzo de 2014, la revista Newsweek afirmó haberlo desenmascarado de forma definitiva: Satoshi Nakamoto era... Dorian Prentice Satoshi Nakamoto, un desaliñado ingeniero de 64 años, residente en California, desempleado, con problemas de salud y coleccionista de trenes en miniatura¹². Este hombre Dorian, catapultado a una incómoda fama, negó ser el creador de Bitcoin –que llamaba Bitcom– y dijo que, de haberlo sido, jamás hubiera utilizado su nombre verdadero¹³. En los foros *online*, después de años de inactividad, brevemente reapareció el Satoshi original negando a su vez ser Dorian¹⁴.

Sea quien fuere, quizás este misterio sea uno de los pilares mismos de Bitcoin. Alejarse del modelo de liderazgo personalista forma parte integral de los principios que el proyecto pretende enarbolar: descentralización, privacidad y desarrollo por consenso. Permite poner en primer plano la idea, el mecanismo y la comunidad, y no distraerse con una biografía, personalidad o afiliación. El mito puede más que el hombre. Como dice la Kena Upanishad: “Saber es no saber, no saber es saber”¹⁵.

2.3 La arquitectura de Bitcoin

En *Bitcoin: A Peer-to-Peer Electronic Cash System*, Nakamoto decía: “Lo que se necesita es un sistema de pagos electrónico que se base en pruebas criptográficas en vez de confianza, permitiendo que dos partes cualquiera, siempre y cuando estén dispuestas, realicen transacciones entre sí de forma directa sin tener que contar con un tercero de confianza”¹⁶. De esta manera, Bitcoin venía a solucionar los problemas del modelo basado en la confianza de los sistemas de pagos tradicionales: la reversibilidad de las transacciones, la posibilidad de fraude y los costos de depender de las instituciones financieras como intermediarias del intercambio electrónico. En plena crisis financiera global de 2008-09, con el crecimiento de la

[10] WALLACE, BENJAMIN. *The rise and fall of Bitcoin*, en Wired, 23 de noviembre de 2011. Acceso online: http://www.wired.com/magazine/2011/11/mf_bitcoin/

[11] *Satoshi Nakamoto is (probably) Nick Szabo*, en Like In A Mirror, 1 de diciembre de 2013. Acceso online: <https://likeinamirror.wordpress.com/2013/12/01/satoshi-nakamoto-is-probably-nick-szabo/>; GILBERT, DAVID. *Who is Satoshi Nakamoto? Bitcoin's Mysterious Creator Revealed as Nick Szabo*, en International Business Times, 3 de diciembre de 2013. Acceso online: <http://www.ibtimes.co.uk/satoshi-nakamoto-nick-szabo-bitcoin-creator-revealed-527078>; VIGNA, PAULA. *Bitcoin Creator Satoshi Nakamoto Unmasked-Again?*, en The Wall Street Journal, 16 de abril de 2014. Acceso online: http://blogs.wsj.com/moneybeat/2014/04/16/bitcoin-creator-satoshi-nakamoto-unmasked-again/?mod=trending_now_4

[12] MC GRATH GOODMAN, LEAH. *The Face Behind Bitcoin*, en Newsweek, 6 de marzo de 2014. Acceso online: <http://mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html>

[13] HERN, ALEX. *Dorian Nakamoto unconditionally denies being the creator of Bitcoin*, en The Guardian, 17 de marzo de 2014. Acceso online: <http://www.theguardian.com/technology/2014/mar/17/dorian-satoshi-nakamoto-denies-creator-bitcoin>

[14] FUNG, BRIAN. *The real-life Satoshi Nakamoto denies being involved in Bitcoin*, en The Washington Post, 6 de marzo de 2014. Acceso online: <http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/06/the-real-life-satoshi-nakamoto-denies-being-involved-in-bitcoin/>

[15] KENA UPANISHAD. English Translation. Acceso online: <https://myweb.space.wisc.edu/jrblack/web/SKT/PDF/Upanishads/roerkenaeng.pdf>

[16] NAKAMOTO, SATOSHI. Op. Cit.

desconfianza hacia los bancos, esto no pasó desapercibido. ¿Cuál era la propuesta? Nakamoto no sólo echó mano del arsenal disponible de conceptos y herramientas, sino que también introdujo nuevos y brillantes elementos para que *Bitcoin* sorteara dos obstáculos que, hasta ese momento, habían sido insalvables para las monedas virtuales: el robo y la falsificación.

2.3.1 El problema del robo

¿Cómo evitar que una persona se apropie de *bitcoins* ajenos y realice transacciones con ellos? Para superar este problema, Nakamoto incorporó un sistema de llaves o

claves criptográficas públicas y privadas para realizar firmas digitales. De modo simplificado, una transacción entre A y B se realiza como explica la *Tabla 1*.

Cuando C le compra a B, se activa el mismo mecanismo, por lo que queda una cadena de registros que verifica la historia de la propiedad de cada *bitcoin*. “Definimos una moneda electrónica como una cadena de firmas digitales”, afirmó Nakamoto.

¿Cómo explicar, entonces, diversos incidentes de robo de *bitcoins* que se han producido en los últimos años?

TABLA 1

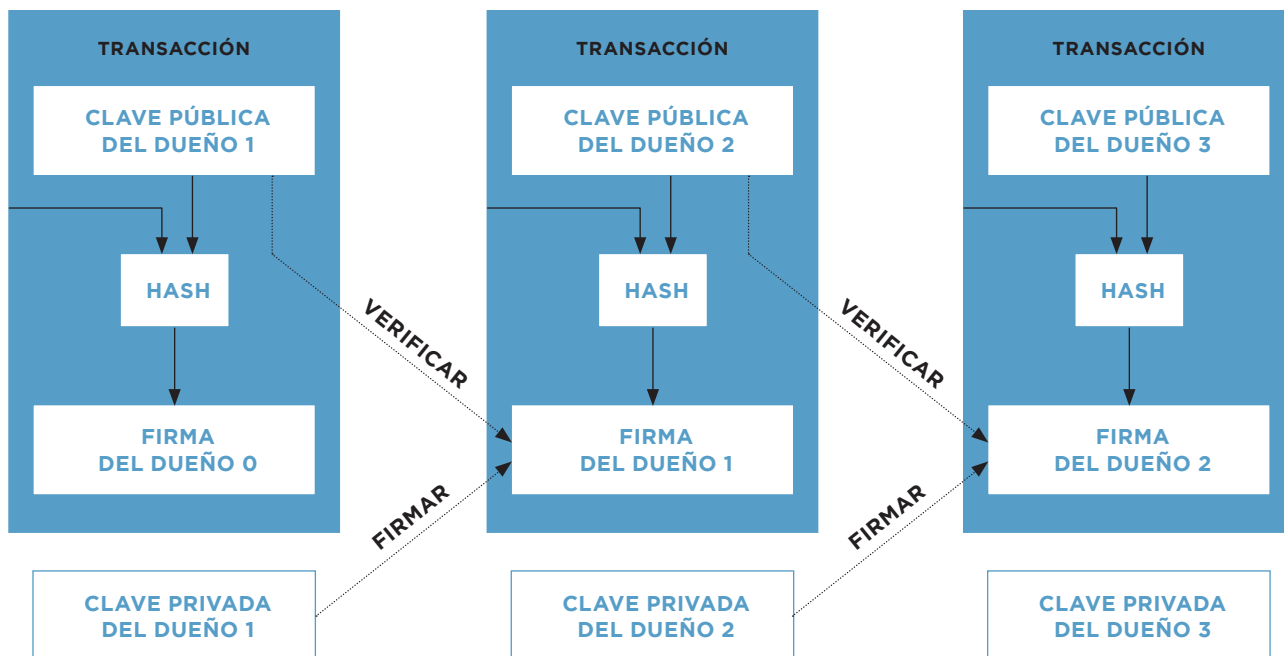
¿Cómo es una transacción de *bitcoin*?¹⁷

Billeteras y direcciones	Para realizar una transacción, tanto A como B deben tener el <i>software</i> correspondiente, es decir, una billetera de <i>Bitcoin</i> instalada en sus computadoras o dispositivos móviles, o una que opere en la red.
	Diversas empresas que ofrecen servicios de billetera, siendo algunas de las más conocidas Blockchain.info, Coinbase, GreenAddress.it, Armory, Mycelium, Circle y Xapo. Cada usuario elige la billetera que más se ajusta a sus necesidades.
	Este <i>software</i> permite crear múltiples direcciones de <i>Bitcoin</i> . Éstas funcionan como claves públicas y tienen asociadas una única clave privada.
	La clave pública es una serie de 34 caracteres (letras y números) generados al azar, por ejemplo: R3LuMExyJ36inYB6712KLC5uteCWhviPy5
	La clave privada tiene la misma estructura, pero sólo es conocida por el dueño de la clave pública.
	Este formato implica que no hay un vínculo directo entre las direcciones y las identidades del mundo real de sus dueños.
	A modo de analogía: si <i>Bitcoin</i> fuera una alcancía, la clave pública sería la ranura y la clave privada sería la llave para abrir la caja y acceder al dinero.
Transacción entre A y B	Supongamos que B le quiere comprar <i>bitcoins</i> a A.
	Primero, B crea una nueva dirección y se la comunica a A.
	A hace un pedido de transacción al sistema. Coloca la clave pública de B (dirección destino) y la cantidad de <i>bitcoins</i> que desea transferirle (monto).
	A firma la transacción con la clave privada de la dirección desde la cual transfiere los <i>bitcoins</i> (dirección origen). De este modo, queda demostrado que A autorizó la transacción.
	¿Cómo obtuvo A sus <i>bitcoins</i> en un principio? Existen diversas posibilidades. Pudo haberlos comprado, por ejemplo, a un particular o en un sitio de <i>trading</i> de <i>Bitcoin</i> , o pudo habérselos ganado en el proceso de minería.

[17] Elaboración propia en base a NAKAMOTO, SATOSHI. Op. Cit.

CUADRO 1

Transacciones con firmas digitales¹⁸



Fuente: Satoshi Nakamoto. Traducción. *Bitcoin.org*

Aquí hay que diferenciar entre la seguridad del protocolo de *Bitcoin* en sí y el mal uso o descuido que puedan tener los usuarios y las instituciones del ecosistema asociado¹⁹.

Según Diego Gutiérrez Zaldívar de Fundación *Bitcoin* Argentina, el principal aprendizaje de la comunidad *Bitcoin* a partir del incidente de Mt Gox, por ejemplo, fue el haber tomado mayor consciencia de que “*el atributo de seguridad del Bitcoin sólo existe si los fondos están protegidos por el libro contable del Bitcoin (Blockchain) y que cuando uno entrega los fondos a un tercero como es el caso de los Exchanges (Bolsas) se aplican las mismas reglas que en el mundo financiero tradicional donde la reputación y la transparencia (por medio de auditorías financieras y de seguridad) son indispensables*”²⁰. De todos modos, hay intentos por mejorar la seguridad del propio sistema, por ejemplo, incorporando un esquema de múltiples claves privadas en vez de dos²¹.

[18] NAKAMOTO, SATOSHI. Op. Cit. Traducción de Angel León. Acceso online: https://bitcoin.org/bitcoin_es_latam.pdf.

[19] HERN, ALEX. *A History of Bitcoin Hacks*, en *The Guardian*, 18 de marzo de 2014. Acceso online: <http://hereisthecity.com/en-gb/2014/03/19/a-history-of-bitcoin-hacks/>; SHARKEY, TOM. *The 7 Biggest Crypto Scandals of 2014*, en *Coindesk*, 26 de diciembre de 2014. Acceso online: <http://www.coindesk.com/7-biggest-crypto-scandals-2014/>; KREITER, MARCY. *Bitstamp Suspends Operations After \$5M Breach Acknowledged*, en *International Business Times*, 5 de enero de 2015. Acceso online: <http://www.ibtimes.com/bitstamp-suspends-operations-after-5m-breach-acknowledged-1774066>.

[20] GUTIÉRREZ ZALDÍVAR, DIEGO. *Fundación Bitcoin Argentina*. Entrevista, 12 de abril de 2014.

[21] Ver, por ejemplo: <https://www.bitgo.com/>.

2.3.2 El problema de la falsificación

La capacidad de replicación de Internet suele considerarse un atributo positivo ya que se puede copiar y enviar todo tipo de archivos –música, videos, textos– sin perder acceso al original. Sin embargo, este espectacular poder multiplicativo no pareciera favorable para una moneda porque, en una suerte de falsificación, se podría copiar y gastar varias veces. Esto se conoce como el *problema del doble gasto*.

La solución clásica es que una autoridad central tenga registro de todas las transacciones para identificar un doble gasto, pero esto es justamente lo que Nakamoto quería evitar. Con ese esquema “*el destino de todo el sistema monetario depende de la compañía que gestiona la casa de moneda*”, afirmó. ¿Cómo hacer, entonces, para verificar que el *bitcoin* que uno compra no ha sido usado ya en otra transacción? “*La única forma de confirmar la ausencia de una transacción es estando al tanto de todas las transacciones [...] Para lograr esto sin un tercero de confianza, las transacciones deben ser anunciadas públicamente; necesitamos un sistema de participantes que estén de acuerdo con una única historia del orden en que éstas fueron recibidas*”²². Este razonamiento encontró su expresión técnica en el *Blockchain* o cadena de bloques, una de las mayores singularidades de *Bitcoin*.

La cadena de bloques es un registro masivo, inalterable y permanente de las transacciones de *bitcoins*. Opera como sistema de contabilidad pública compartida en una red P2P en la que los propios usuarios son responsables de la validación de las transacciones. Se puede agregar nuevos datos pero no removerlos, ya que cada transacción que se incorpora contiene el rastro de todas las anteriores, actuando como cápsula de ADN histórico financiero. Todos los usuarios de *Bitcoin* tienen una copia personal de la cadena completa que se alarga con el paso del tiempo.

A su vez, el *Blockchain* constituye la solución al Problema de los Generales Bizantinos, un problema histórico de las ciencias de la computación. Conceptualmente, se plantea del siguiente modo: diversos generales que sólo pueden comunicarse por medio de mensajeros deben encontrar la manera de llevar adelante un ataque coordinado pese a la profunda desconfianza que se tienen unos a otros²³. En el caso de *Bitcoin*, sería preguntarse cómo hacen millones de nodos de una red, que no se conocen entre sí –y que por lo tanto no tienen por qué confiar en los demás– para ponerse de acuerdo sobre el historial válido de las transacciones. La respuesta se encuentra en un proceso llamado *minería* que es simultáneamente:

- El mecanismo de validación de las transacciones de *bitcoins* (2.3.2.1).
- El mecanismo de creación de nuevos *bitcoins* (2.3.2.2).

Se ha dicho que la mejor manera de describir la minería es “*una cruzada entre la Lotería y la Fiebre del Oro de California*”²⁴. Lotería porque la validación de las transacciones tiene un alto componente de azar, y Fiebre del Oro porque los mineros, en una enardecida competencia, buscan hacerse ricos en un proceso análogo al de mediados del siglo XIX.

[22] NAKAMOTO, SATOSHI. Op. Cit.

[23] LAMPORT, LESLIE, et al. *The Byzantine Generals Problem*, en ACM Transactions on Programming Languages and Systems, Vol. 4, N° 3, Julio de 1982. Acceso online: <http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf>; ANDREESSEN, MARK. *Why Bitcoin Matters*, en The New York Times, 21 de enero de 2014. Acceso online: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1.

[24] *Bitcoin Mining*, en Butterfly Labs. Acceso online: <http://www.butterflylabs.com/bitcoin-mining/>.

2.3.2.1 La minería (I): Validación de las transacciones

TABLA 2
¿Cómo se validan las transacciones de bitcoin? El proceso de minería

Objetivo	Uno de los objetivos de la minería es confirmar la validez de las transacciones de <i>bitcoins</i> para evitar el problema del doble gasto.
	Cuando A y B realizan una transacción, el detalle de la misma es enviado a la red <i>Bitcoin</i> donde es recogido por los mineros para ser validado.
	Cada minero incluye los datos de la transacción en un bloque que se define como el conjunto de transacciones realizadas en los últimos 10 minutos.
	La idea es que ese bloque quede incluido en la cadena de bloques que es el registro histórico público de todas las transacciones válidas.
Los mineros	Los mineros son personas, grupos o entidades que ponen a disposición la capacidad de procesamiento de sus CPU, GPU (<i>Graphics Processing Unit</i>), FPGA (<i>Field-Programmable Gate Array</i>) o ASIC (<i>Application-Specific Integrated Circuit</i>) con el fin de resolver complejos cálculos matemáticos requeridos para incorporar un bloque a la cadena.
	Cualquiera puede ser minero si así lo deseara.
	El incentivo para dedicarse a la minería es que, si se logra incorporar un bloque a la cadena, el sistema otorga una recompensa de <i>bitcoins</i> .
Datos del bloque	Cada bloque tiene un header o cabecera que condensa información sobre 3 elementos (<i>ver figura</i>).
	Hash Raíz: es un <i>hash</i> que contiene la información sobre las transacciones contenidas en el bloque mismo. Éstas son las transacciones que se desean validar (el <i>hash</i> es producido por los mineros mediante un Árbol de Merkle).
	Hash Previo: es un <i>hash</i> que contiene la información sobre el último bloque considerado válido que, a su vez, contiene la información sobre todos los bloques anteriores validados por la red.
	Nonce: un <i>nonce</i> que es un número generado al azar.
	Bloque <pre>graph TD subgraph "CABECERA DE BLOQUE (HASH DEL BLOQUE)" HP[HASH PREVIO] N[NONCE] HR[HASH RAÍZ] end HR --> H01[HASH01] HR --> H23[HASH23] H01 --> H0[HASH0] H01 --> H1[HASH1] H23 --> H0[HASH0] H23 --> H1[HASH1] H0 --> Tx0[Tx0] H1 --> Tx1[Tx1] H0 --> Tx0[Tx0] H1 --> Tx1[Tx1]</pre> Fuente: Satoshi Nakamoto. Traducción. <i>Bitcoin.org</i>²⁵

[25] NAKAMOTO, SATOSHI. Traducción de Angel León. Op. Cit.

¿Cómo se validan las transacciones de *bitcoin*? El proceso de minería

BOLETÍN INFORMATIVO TECHINT 348

TABLA 2 (CONTINUACIÓN)

¿Cómo se validan las transacciones de *bitcoin*? El proceso de minería

Confirmación final	Si un atacante quisiera cambiar o eliminar una transacción que ya se encuentra en la cadena de bloques, su accionar generaría un cambio inmediato en el Elemento 1 (<i>Hash Raíz</i>) del bloque intervenido y, por lo tanto, en el <i>hash</i> identificativo de ese bloque.
	Sin embargo, supongamos que dicho atacante logra obtener un <i>nonce</i> que, junto con el <i>Hash Raíz</i> alterado, genera un <i>hash</i> identificativo adecuado. Este bloque fraudulento, ¿podría ser aceptado por la red? La respuesta es no.
	Como el <i>hash</i> de cada bloque sirve como insumo para el <i>header</i> del bloque siguiente, un cambio provoca una alteración en todos los bloques posteriores (si se cambia el <i>hash</i> del bloque 50, cambia el <i>hash</i> del bloque 51, 52, 53, etc.). Es así que el atacante tendría que volver a encontrar un <i>hash</i> para todos los bloques posteriores al que manipuló, lo que podría durar semanas, meses y hasta años.
	Por otra parte, el resto de la red seguiría funcionando con normalidad, agregando nuevos bloques a la cadena mucho más rápido que el atacante. Como la red acepta como válida la cadena que tiene mayor prueba de trabajo invertida en ella, finalmente prevalece la cadena legítima sobre la fraudulenta.
	Sólo podría crearse una cadena ilegítima si alguien tuviera bajo su control la mayoría (51%) de la potencia de procesamiento de la red.
	Hoy en día esto es altamente improbable. En noviembre de 2013 la red <i>Bitcoin</i> superó la capacidad de las 500 principales supercomputadoras del mundo multiplicada más de 200 veces. Esto explica parte del lema de <i>Bitcoin Vires in Numeris</i> o <i>La fuerza en los números</i> .
	Un atacante que tuviera el 10% del poder de procesamiento de la red tendría una probabilidad del 0,024% de ganarle a la red durante la creación de 6 bloques consecutivos. Por eso, se recomienda esperar a que se produzcan 6 bloques –en la jerga, 6 confirmaciones– para considerar que la transacción ha sido confirmada por completo, sobre todo si se trata de grandes sumas de dinero ²⁶ .

[26] Agradecimiento especial: Manuel Beaudroit, Nubis Bruno y Tomás Rojas de Bitex.la.

Fuentes: NAKAMOTO, SATOSHI. Op. Cit.; *How a Bitcoin transaction works*, Op. Cit.; y *Bitcoin Economy*, Infografía. Acceso online: <http://blog.thomsonreuters.com/wp-content/uploads/2014/02/bitcoin.jpg>; *How Bitcoin Mining Works*, en Coindesk. Acceso online: <http://www.coindesk.com/information/how-bitcoin-mining-works/>; *¿Cómo funciona Bitcoin?*, en Bitcoin.org. Acceso online: <https://bitcoin.org/es/como-funciona>; *Wiki de Bitcoin*. Acceso online: https://es.bitcoin.it/wiki/P%C3%A1gina_principal; *¿Qué es Bitcoin? Una sencilla introducción*, Acceso online: <http://www.queesbitcoin.info/>; Szabo, Nick. *Trusted Third Parties Are Security Holes*, Acceso online: <http://szabo.best.vwh.net/https.html>; PACIA, CHRIS. *Bitcoin Mining Explained Like You're Five: Part 2*, en Escape Velocity. Acceso online: <http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/>.

No obstante, en los últimos tiempos se ha generado cierta preocupación en torno a dos cuestiones:

- **La centralización de la minería:** en junio de 2014 el *pool* minero GHash.IO superó la brecha del 50% del poder de procesamiento por más de 12 horas, por lo que estuvo en la posición de lanzar un denominado *ataque del 51%* si lo hubiera querido. Aunque los representantes del *pool* afirmaron que jamás llevarían a cabo un ataque de este estilo, sería paradójico que *Bitcoin*, nacido para desterrar el *problema de la confianza*, terminara dependiendo de la confianza de los participantes en los *pools* de minería²⁷.
- **El incentivo del minero egoísta:** otra preocupación es el llamado *incentivo del minero egoísta* que consiste en la colusión de diversos mineros en carteles para obtener más ingresos de lo que les correspondería por su poder de procesamiento, a expensas de los mineros honestos. En este sentido, para el correcto funcionamiento del sistema, se necesitaría un umbral superior al 50%, más cercano al 75%²⁸.

[27] Ver: EYAL, ITTAY y GUN SIRER, EMIN. *It's Time For a Hard Bitcoin Fork*, en Hacking, Distributed, 13 de junio de 2014. Acceso online: <http://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/>; KERYA, ALEX. *GHash.IO is open for discussion*, en Official CEX.IO Blog, 16 de junio de 2014. Acceso online: <http://blog.cex.io/ghash-io-51-percent/>; ANDRESEN, GAVIN. *Centralized Mining, Bitcoin Foundation Blog*, 13 de junio de 2014. Acceso online: <https://bitcoinfoundation.org/blog/>.

[28] Ver: EYAL, ITTAY y GUN SIRER, EMIN. *Majority is not Enough: Bitcoin Mining is Vulnerable*, en ArXiv. Acceso online: <http://arxiv.org/pdf/1311.0243v5.pdf>; BUTERIN, VITALIK. *Selfish Mining: A 25% Attack Against the Bitcoin Network*, en Bitcoin Magazine, 4 de noviembre de 2013. Acceso online: <http://bitcoinmagazine.com/7953/selfish-mining-a-25-attack-against-the-bitcoin-network/>; HEILMAN, ETHAN. *One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner*, en Cryptology ePrint Archive. Acceso online: <https://eprint.iacr.org/2014/007.pdf>.

[29] HAJDARBEGOVIC, NERMIN *Bitcoin Price Decline Sparks Rare Mining Difficulty Drop*, en Coindesk, 3 de diciembre de 2014. Acceso online: <http://www.coindesk.com/bitcoin-price-decline-sparks-rare-mining-difficulty-drop/>.

2.3.2.2. La minería (II): Creación de nuevos bitcoins

Como el proceso descrito es tan complejo, el sistema ofrece una interesante recompensa al minero: la posibilidad de *minar* o *extraer* para sí nuevos *bitcoins*. Esto sucede cuando logra incorporar un nuevo bloque a la cadena. De esta manera, los mineros son quienes obtienen el beneficio del *señoreaje* que, en el sistema de dinero fiduciario, le corresponde al Banco Central por tener el monopolio de emisión de la moneda. La rentabilidad final que obtienen los mineros depende de varios factores, entre ellos: el costo de la electricidad, la cantidad de *bitcoins* obtenida y su cotización, y el costo de los equipos, su capacidad de procesamiento y su velocidad de depreciación.

Sin embargo, hay que tener en cuenta que la capacidad de obtener nuevos *bitcoins* no se prolongará por tiempo indefinido. Esto se debe al propio diseño de *Bitcoin* que contempla una creación de bloques constante y recompensas cada vez menores para los mineros.

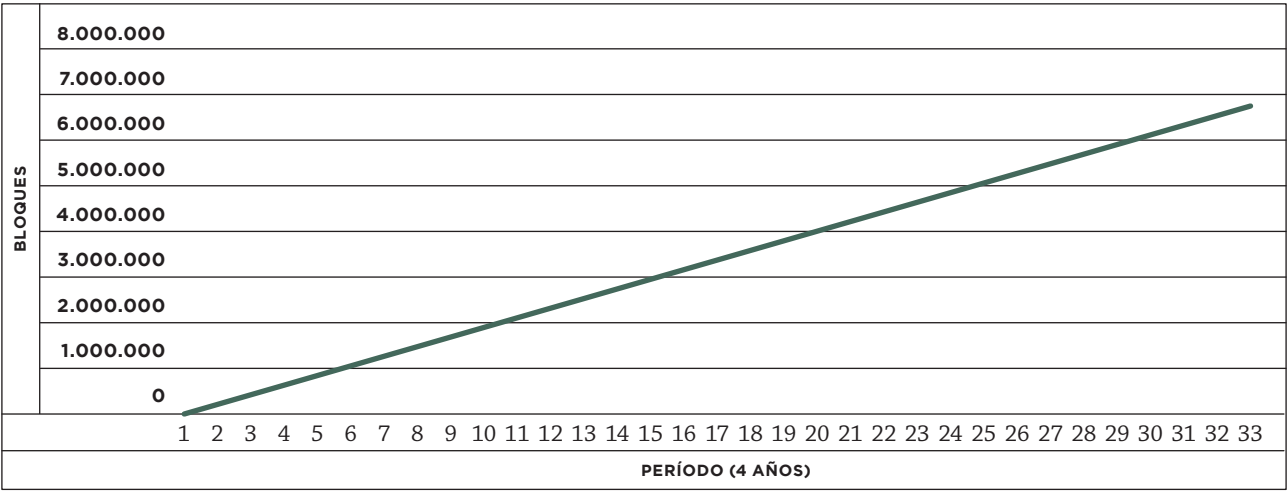
En primer lugar, el sistema tiene un modo de autorregulación para que se produzca un nuevo bloque cada 10 minutos en promedio, es decir, 210.000 bloques cada 4 años. Esto se logra ajustando el *target* de dificultad cada 2.016 bloques, según la cantidad de mineros en el sistema. A mayor cantidad de mineros, mayor probabilidad de resolver los bloques, por lo que el sistema eleva el nivel de dificultad; y viceversa. En diciembre de 2014 se produjo la primera declinación en la dificultad desde la creación de Bitcoin²⁹.

La *Tabla 3* y los *Gráficos 1* y *2* ilustran esta particularidad.

TABLA 3

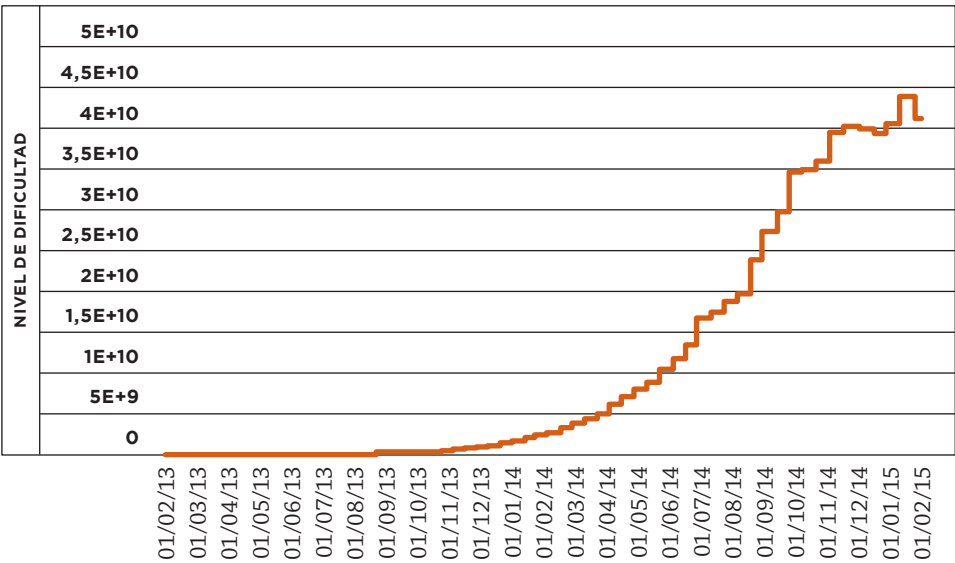
Período	Años	Bloques creados	Bloques al inicio del periodo	Bloques al final del periodo
1	2009-2012	210.000	0	210.000
2	2013-2016	210.000	210.000	420.000
3	2017-2020	210.000	420.000	630.000
4	2021-2024	210.000	630.000	840.000
5	2025-2028	210.000	840.000	1.050.000

GRÁFICO 1
Creación de bloques constante



Fuente: Elaboración propia.

GRÁFICO 2
Cambiante nivel de dificultad en la creación de bloques
Feb. 2013- Feb. 2015³⁰



[30] Dificultad, en Blockchain.info. Acceso online: https://blockchain.info/es/charts/difficulty?timespan=all&showDataPoints=false&daysAverageString=1&show_

Fuente: Elaboración propia en base a Blockchain.info

En segundo lugar, el sistema tiene un mecanismo de recompensas decrecientes para los mineros. En un principio, el premio por bloque era de 50 *bitcoins*, ahora es de 25 *bitcoins*, y el monto reduce un 50% cada 4 años o cada 210.000 bloques. En los primeros años se observa:

TABLA 4

Período	Años	Recompensa por bloque
1	2009-2012	50
2	2013-2016	25
3	2017-2020	12,5
4	2021-2024	6,25
5	2025-2028	3,125

Fuente: Elaboración propia.

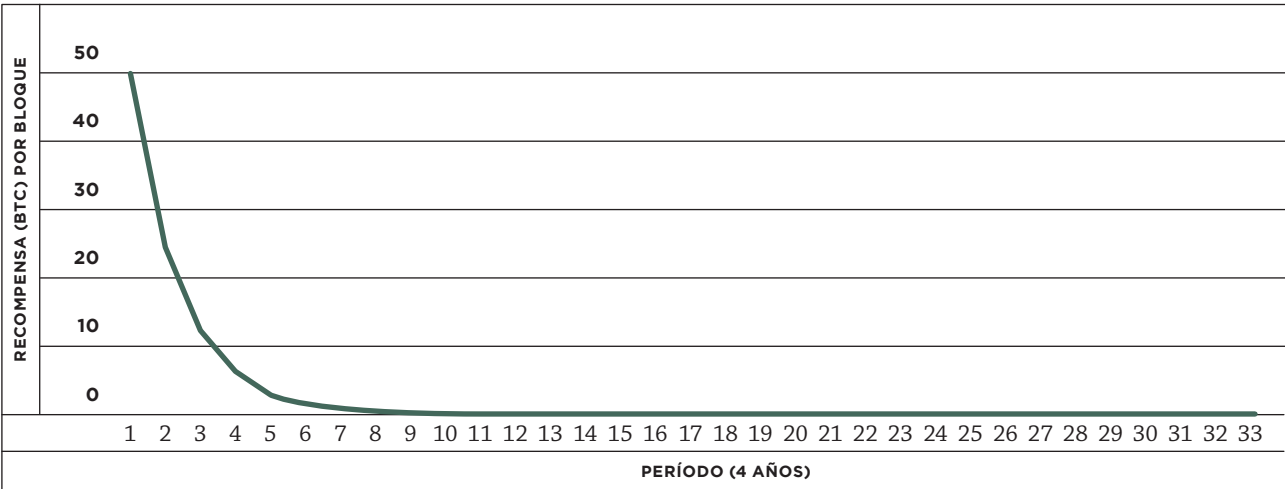
[31] Al 1 de febrero de 2015 había 13,8 millones. Ver: *Total de Bitcoins en circulación* en Blockchain.info. Acceso online: <https://blockchain.info/es/charts/total-bitcoins>.

Pareciera que, a medida que pasa el tiempo, el incentivo de minar se vuelve cada vez menor. ¿Esto significará el fin de la minería? La respuesta es no. Cuando la recompensa sea ya muy pequeña, los usuarios podrán incluir una comisión o *fee* para quienes resuelvan el bloque en el que aparece su transacción. El monto de esas comisiones será determinado por la interacción entre los mineros y los usuarios. Por lo tanto, seguirá existiendo incentivo para la minería.

Tomados en conjunto, estos dos factores –creación de bloques constante y recompensas decrecientes– significan que la cantidad de nuevos *bitcoins* se irá reduciendo cada vez más hasta llegar a un techo de 21 millones de unidades, límite que se alcanzaría alrededor del año 2140. Estrictamente, como la creación de nuevos *bitcoins* se reduce a la mitad cada 4 años, hay una aproximación asintótica a ese límite. Lo que sucede es que, cuando el incremento en *bitcoins* sea menor que 1 satoshi (0,00000001 BTC), la mínima subunidad de *Bitcoin*, ya no será posible contabilizar los aumentos, por lo que se considera que se habrá llegado a los 21 millones. En la actualidad, hay unos 14 millones de *bitcoins* en circulación³¹.

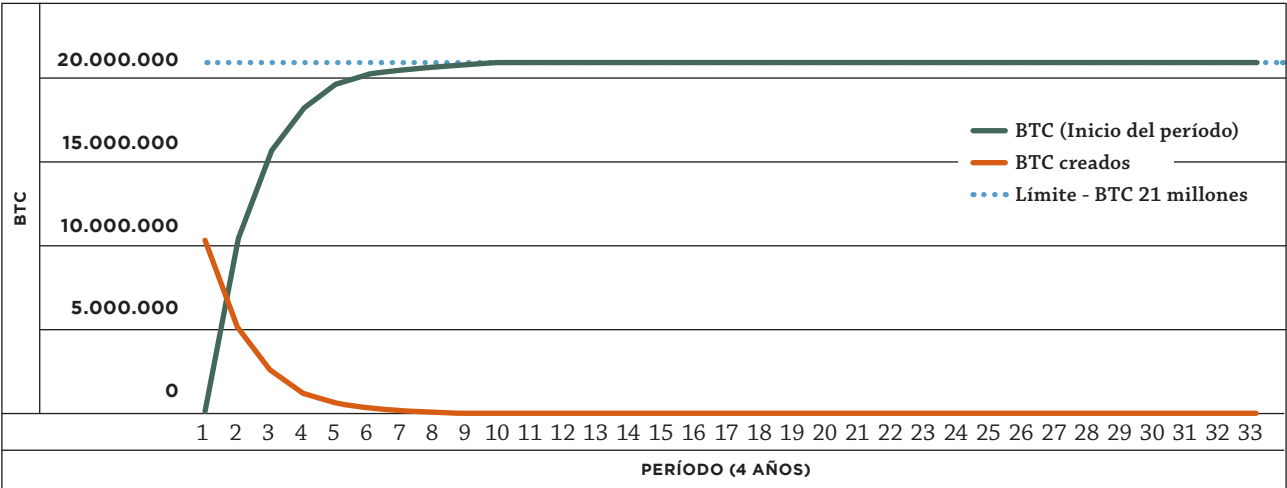
GRÁFICO 3

Recompensa (BTC) por bloque



Fuente: Elaboración propia.

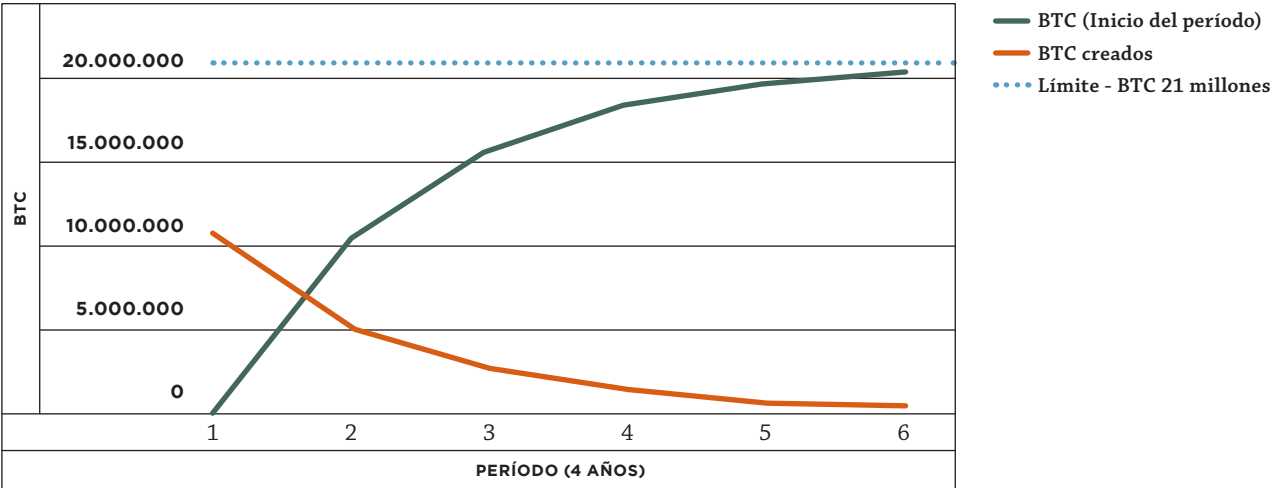
GRÁFICO 4
Bitcoins (BTC) en circulación - 2009-2140



Fuente: Elaboración propia.

Haciendo foco en los primeros años se observa:

GRÁFICO 5
Bitcoins (BTC) en circulación - 2009-2024



Fuente: Elaboración propia.

2.4 Atributos de Bitcoin

Las explicaciones sobre el funcionamiento de *Bitcoin* son esenciales porque es justamente su arquitectura la que le confiere sus principales atributos:

TABLA 5

Atributos de Bitcoin

Existencia virtual	<i>Bitcoin</i> tiene una existencia puramente virtual.
	No tiene una existencia material, correlato o respaldo en el mundo real. No es una versión electrónica del dinero fiduciario y no tiene curso legal en ninguna jurisdicción. Sin embargo, no está circunscripto a un espacio virtual cerrado, sino que puede ser intercambiado por monedas fiduciarias, bienes y servicios.
	El protocolo de <i>Bitcoin</i> está diseñado de modo tal que, en términos estrictos, no existen <i>bitcoins</i> como tal en el ciberespacio, sino balances de <i>bitcoins</i> y registros de transacciones entre distintas direcciones.
Emisión descentralizada y predeterminada	La emisión de <i>bitcoins</i> está determinada por el protocolo. No depende de un Banco Central o de ninguna otra institución central con criterio discrecional.
	A través del proceso de minería, se crean nuevos <i>bitcoins</i> a un ritmo decreciente hasta llegar a una oferta total de 21 millones de unidades en el año 2140. Esto significa que la oferta de <i>bitcoins</i> es conocida en todo momento, mientras que la demanda fluctúa y depende de diversos factores.
	La unidad más pequeña del <i>Bitcoin</i> es 1 satoshi, o 0,00000001 BTC. Potencialmente, podrían agregarse más decimales en el futuro.
	Los mineros son quienes obtienen el beneficio del señoreaje.
	El diseño de <i>Bitcoin</i> implica que no hay un sistema de reserva fraccionaria. Se asemeja a una economía de efectivo puro.
Validación de las transacciones descentralizadas	La validación de las transacciones de <i>Bitcoin</i> se realiza a través de una red descentralizada P2P de mineros y no por una institución o intermediario.
	Esto es posible gracias al Blockchain o cadena de bloques, el libro contable público distribuido que funciona como registro histórico de todas las transacciones de <i>Bitcoin</i> .
Sistema pseudónimo	<i>Bitcoin</i> opera en base a un sistema pseudónimo que ofrece una potente combinación de transparencia y privacidad.
	Transparencia, porque las transacciones quedan registradas en la cadena de bloques (que es pública) asociadas a las claves públicas de los usuarios.
	Privacidad, porque las claves públicas, combinaciones de 34 caracteres de números y letras, no se encuentran ligadas a las identidades de la vida real de los usuarios.
Alcance global	Se pueden realizar transacciones de <i>Bitcoin</i> en cualquier parte del planeta, a nivel nacional e internacional, sin pasar por los canales tradicionales de intermediación financiera, siempre que se tenga conexión a Internet.

Visto esto, conviene mirar de cerca la evolución de *Bitcoin* desde su creación.

2.5 El año de...

A grandes rasgos, la evolución de *Bitcoin* por año podría caracterizarse del siguiente modo:

TABLA 6

Los años de *bitcoin*

2009 El año del inicio	Satoshi Nakamoto <i>minó</i> el primer bloque de <i>Bitcoin</i> , <i>el bloque genesis</i> , y el 12 de enero se produjo la primera transacción, entre Nakamoto y Hal Finney ³² .
	En esta etapa, los usuarios, básicamente entusiastas de la criptografía, intercambiaban <i>bitcoins</i> a valor casi nulo.
2010 El año de la pizza	Se produjo la primera transacción de <i>Bitcoin</i> para comprar un objeto real cuando el usuario Lazlo ofreció BTC 10.000 a cambio de 2 pizzas.
	En este año Mt Gox se lanzó como plataforma para intercambiar <i>bitcoins</i> por otras monedas.
	Se detectó un problema en el protocolo que permitía incluir transacciones no verificadas en la cadena de bloques. Esta vulnerabilidad fue corregida.
2011 El año del murmullo	<i>Bitcoin</i> comenzó a ganar una incipiente visibilidad en los medios y en junio de 2011 Wikileaks empezó a aceptar donaciones de <i>Bitcoin</i> .
	En febrero, la cotización del BTC alcanzó la paridad 1 a 1 con el USD. En julio el precio del <i>Bitcoin</i> alcanzó los USD 31, el pico de la primera <i>burbuja</i> , y en diciembre alcanzó un mínimo de USD 2.
2012 El año de la consolidación	Wordpress comenzó a aceptar <i>Bitcoin</i> , como así también otras empresas menos conocidas de diversos rubros (por ejemplo, taxis, música y salud). Se produjo el primer juicio que involucraba a <i>Bitcoin</i> y se enseñó la primera clase sobre <i>Bitcoin</i> en una escuela pública.
	El precio fue creciendo hasta alcanzar USD 13 en diciembre.
2013 El año de la ilusión	El precio subió hasta USD 100 el 1 de abril y USD 266 el 11 de abril por la crisis económica de Chipre que incluyó un rescate internacional, un corralito bancario, restricciones al movimiento de capitales y creciente desconfianza hacia el sistema bancario ³³ .
	En agosto, el término <i>Bitcoin</i> fue incorporado a <i>Oxford Dictionaries Online</i> (junto con <i>twerk</i> y <i>selfie</i>) como una <i>moneda digital cuyas transacciones se pueden realizar sin la necesidad de un banco central</i> ³⁴ .
	En octubre, el FBI cerró Silk Road, un sitio de compra y venta de drogas que usaba <i>Bitcoin</i> para sus transacciones.

[32] *Is Bitcoin the Future of Money*. Acceso online: <http://www.mapsofworld.com/poll/is-bitcoin-the-future-of-money-facts-infographic.html>.

[33] COX, JEFF. *Bitcoin Bonanza: Cyprus Crisis Boosts Digital Dollars*, en CNBC, 27 de marzo de 2013. Acceso online: <http://www.cnbc.com/id/100597242>; MUSIL, STEVEN. *Bitcoin hits record exchange values with Cyprus banking crisis*, en CNET, 28 de marzo de 2013. Acceso online: <http://news.cnet>.

com/8301-1023_3-57576928-93/bitcoin-hits-record-exchange-values-with-cyprus-banking-crisis/; COLAS, NICHOLAS. *Bitcoin: Spirits in the Material World*, en Tabb Forum, 22 de marzo de 2013. Acceso online: <http://tabbforum.com/opinions/bitcoin-spirits-in-the-material-world>.

[34] *Language review 2013: from bitcoin to sharknado*, Acceso online: <http://blog.oxforddictionaries.com/2013/11/language-review-2013/>.

TABLA 6 (CONTINUACIÓN)

Los años de bitcoin

2013 El año de la ilusión	Desde principios de octubre, los comentarios positivos de Ben Bernanke, el entonces Presidente de la Fed de EEUU, junto con el crecimiento de la demanda de China, impulsaron hacia arriba el precio: pasó de USD 203 el 1 de noviembre a USD 1.119 el 30 de noviembre.
	En diciembre, el Banco Popular de China dijo que <i>Bitcoin</i> era un ente <i>sin significado</i> y prohibió su manejo en las instituciones financieras chinas, lo que generó una caída del precio ³⁵ .
2014 El año del replanteo	En febrero se produjo el colapso de Mt Gox, uno de los sitios de intercambio de <i>Bitcoin</i> más importante del mundo. La empresa anunció que había ‘perdido’ 850.000 <i>bitcoins</i> de la empresa y los clientes, valuados entonces en USD 480 millones, y pidió la quiebra. Todavía no se sabe a ciencia cierta qué pasó. Fue la primera vez que la criptomoneda sufría un incidente de tan alto perfil, y se generaron intensos debates en los medios, foros y redes sociales ³⁶ .
	El valor de <i>Bitcoin</i> se depreció aproximadamente un 60% contra el USD, convirtiéndolo en una de las monedas de peor desempeño a nivel global.
	Pese a esto, el ecosistema de <i>Bitcoin</i> siguió creciendo a lo largo del año. Las inversiones de capital de riesgo pasaron de USD 96 millones en 2013 a USD 335 millones en 2014 e importantes empresas anunciaron su aceptación de <i>Bitcoin</i> .
	El fenómeno atrajo la atención de los bancos centrales y gobiernos alrededor del mundo que comenzaron a estudiar y regularlo ³⁷ .

El año 2015 no comenzó de modo auspicioso. Se produjo una importante caída del precio: pasó de USD 315,7 el 1 de enero de 2015 a USD 229 el 31 de enero de 2015, lo que se sumaba a una caída del 17% en diciembre de 2014³⁸. Esto generó diversas especulaciones sobre las causas de esta contracción y hasta se llegó a vaticinar el fin de la criptomoneda. Sumado a eso, en enero Bitstamp, uno de los principales sitio web de intercambio de *bitcoins*, con base en Eslovenia, anunció que había sido víctima de un *hackeo* en el que resultaron robados 19.000 *bitcoins*, equivalente a USD 5 millones a precios del momento. El ataque cibernético no puso en jaque a la empresa ya que el monto robado representaba una parte pequeña de los fondos destinados a las transacciones diarias, pero puso de relieve las vulnerabilidades que todavía tiene el ecosistema asociado a *Bitcoin*.

[35] *Bitcoins tumble in value on China clampdown*, en The Telegraph, 18 de diciembre de 2013. Acceso online: <http://www.telegraph.co.uk/finance/currency/10524614/Bitcoins-tumble-in-value-on-China-clampdown.html>; CLINCH, MATT. *Bitcoin price halves as China clampdown escalates*, en CNBC, 18 de diciembre de 2013. Acceso online: <http://finance.yahoo.com/news/bitcoin-price-halves-china-clampdown-085816934.html>; *China Bans Financial Companies From Bitcoin Transactions* en Bloomberg, 5 de diciembre de 2013. Acceso online: <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html>.

[36] *Almost Half a Billion Worth of Bitcoins Vanish*, en The Wall Street Journal, 28 de febrero de 2014. Acceso online: <http://online.wsj.com/news/articles/SB10001424052702303801304579410010379087576>; KNIGHT, SOPHIE y LAYNE, NATHAN. *Exclusive: Mt. Gox faced questions on handling client cash long before crisis*, en Reuters, 29 de marzo de 2014. Acceso online: <http://www.reuters.com/article/2014/03/30/us-bitcoin-mtgox-idUSBREA2To1T20140330>; DECKER, CHRISTIAN y WATTENHOFER, ROGER. *Bitcoin Transaction Malleability and Mt Gox*, en Cornell University Library, 26 de marzo de 2014. Acceso online: <http://arxiv.org/pdf/1403.6676v1.pdf>.

[37] *State of Bitcoin 2015: Ecosystem Grows Despite Price Decline*, en Coindesk, 7 de enero de 2015. Acceso online: <http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/>.

[38] Blockchain.info.

3. INTERPRETACIONES DE BITCOIN

3.1 Bitcoin como dinero

Bitcoin es conocido popularmente como moneda virtual y los comentaristas suelen juzgar su valor y efectividad en base a esta definición. Sin embargo, cabe preguntarse si el mote de *dinero* es adecuado para describirlo. En las ciencias económicas, ha primado una definición funcionalista del dinero sobre una esencialista, y se dice que es dinero todo aquello que cumple tres funciones:

- > Medio de intercambio (3.1.1)
- > Unidad de cuenta (3.1.2)
- > Reserva de valor (3.1.3)

Bitcoin, ¿las cumple?

3.1.1 Medio de intercambio

La mención del dinero como medio de intercambio puede rastrearse hasta el Libro I de Política de Aristóteles y fue el aspecto más subrayado por la Escuela Clásica que creía en la neutralidad del dinero. Los libros de texto suelen explicar que el dinero surgió para solucionar los inconvenientes del trueque, en particular, el *problema de la doble coincidencia*: para lograr un intercambio exitoso, se debía encontrar a alguien dispuesto a intercambiar el bien o servicio deseado justo por el bien o servicio ofrecido, proceso que podía ser harto complicado. Con la creación del dinero como medio de intercambio, se cambiaba el bien o servicio ofrecido por dinero, y luego con ese dinero se compraba el bien o servicio deseado. Esto ahorra el costo de buscar, muchas veces a lo largo de varias transacciones, a otro que cumpliera el requisito de la *doble coincidencia*. Esta explicación es desafiada por el antropólogo David Graeber quien postula que, históricamente, el dinero no surgió a partir de los inconvenientes del trueque. “La versión estándar de la historia monetaria está al revés. No comenzamos con el trueque, descubrimos el dinero, y después eventualmente desarrollamos sistemas de crédito. Sucedió precisamente al revés”, sostiene³⁹.

Más allá de esta controversia, se dice que un bien funciona como medio de intercambio cuando es aceptado por todos para la compra y venta de bienes y servicios, y para el pago de salarios y deudas. Para ello, es necesario que cumpla varios requisitos. Primero, debe ser fácilmente transportable de modo que sea cómodo para las transacciones cotidianas. En el caso del dinero fiduciario, el efectivo es fácil de llevar en una billetera cuando se trata de sumas pequeñas pero, para montos grandes, hace falta tomar otro tipo de precauciones (por ejemplo, camiones blindados). Las tarjetas de débito y crédito usadas en reemplazo del efectivo son convenientes para transportar pero pueden traer asociados nuevos costos. El dinero electrónico, también sustituto del efectivo, es la alternativa más sencilla en este respecto, pero hay que tener en cuenta que no todos están en el sistema bancario, sobre todo en países en vías de desarrollo⁴⁰. En contraste, *Bitcoin*, al ser virtual, no necesita ser transportado y realizar transacciones es un asunto sencillo siempre y cuando se tenga conexión a Internet.

En segundo lugar, para funcionar como medio de intercambio, es preciso que el dinero sea divisible ya que no todas las transacciones se realizan por números enteros. Como se ha visto, en la actualidad 1 *bitcoin* se subdivide hasta 0,00000001 BTC o 1 satoshi. Si fuera necesario, el protocolo podría modificarse para producir subdivisiones adicionales. La tercera propiedad es la de fungibilidad, es decir, que una unidad (o subunidad) del dinero sea equivalente a cualquier otra en cuanto a valor y aceptación, y que sean reemplazables entre sí. *Bitcoin* también cumple esta característica, aunque esto podría cambiar:

[39] GRAEBER, DAVID. *Debt: The First 5000 Years*. Nueva York: Melville House, 2010.

[40] La experiencia de M-pesa en Kenya es interesante en este sentido. Ver: GRAEBER, CHARLES. *Ten Days in Kenya With No Cash, Only a Phone*, en Bloomberg Businessweek, 5 de junio de 2014. Acceso online: <http://www.businessweek.com/articles/2014-06-05/safaricom-m-pesa-turns-kenya-into-a-mobile-payment-paradise>.

- Hay un debate sobre la creación de un sistema de validación para identificar *bitcoins* robados o usados en actividades ilegales. Esto removería la propiedad de fungibilidad ya que habría una diferencia entre los *bitcoins* buenos y los malos. No obstante, esto todavía está lejos de implementarse⁴¹.
- En algunos casos, como se observa en los foros *online*, los usuarios ofrecen varios *bitcoins* por alguno relacionado al *bloque génesis* o a la primera transacción de *bitcoins* por un bien real (la pizza de Lazlo). Esto le da distintos valores a distintos *bitcoins*.
- Algunas regulaciones, como las del Internal Revenue Service (IRS) de EEUU, rompen la fungibilidad al hacer más rentable gastar unos *bitcoins* que otros.
- Los *Colored Coins*, que *colorean* a los *bitcoins* con atributos específicos, o que los vinculan a activos del mundo real, también romperían la propiedad de fungibilidad.

Por último, el dinero debe tener aceptación generalizada para la compra y venta de productos y servicios. Por el momento, *Bitcoin* no cumple esta condición. Si bien su aceptación ha crecido en los últimos años, dista de ser generalizada. Algunos creen que, hasta que *Bitcoin* no sirva para pagar impuestos o hasta que la Justicia no lo acepte como modo de saldar deudas, sus limitaciones serán claras. Más allá de esto, como sucede con otras monedas, el poder de *Bitcoin* radicará en el poder de la red de individuos y empresas que decidan utilizarlo. Esto explica que uno de los principales intereses de la comunidad *Bitcoin* sea la de *evangelizar* sobre las bondades de la criptomoneda. Su éxito sólo podrá evaluarse con el tiempo.

Uno de los desafíos que enfrenta *Bitcoin* para crecer es la complejidad del sistema para quienes se acercan por primera vez. El hecho de que se encuentre en una etapa experimental, la volatilidad del precio, los recaudos de seguridad exigidos y la falta de garantías ante la pérdida o el *hackeo* hacen que muchos opten por mantenerse en los canales tradicionales. En este aspecto, es fundamental desarrollar mecanismos de educación y protección al consumidor. Por el lado de las empresas, *Bitcoin* es admitido en diversas pági-

nas *web* y comercios alrededor del mundo: hoteles, agencias de viaje, restaurantes, sitios de comercio electrónico, sitios de juegos *online*, servicios profesionales y servicios financieros, entre otros. Algunos de los casos más renombrados son Microsoft, Dell, Expedia, Wordpress, Paypal, Overstock y TigerDirect.

Para negocios con baja capacidad de fijar márgenes de rentabilidad, es especialmente atractiva la falta de comisiones o costos adicionales de *Bitcoin* frente a las tarjetas de crédito, por ejemplo. Sin embargo, muchas de las empresas que aceptan *Bitcoin* técnicamente no se exponen a las fluctuaciones de su valor ya que, por medio de un intermediario, convierten los *bitcoins* a otra moneda de manera inmediata⁴². Según Coinmap, unos 6.221 comercios alrededor del mundo aceptaban *Bitcoin* al 1 de febrero de 2015. Como la página sólo muestra los comercios que se han inscrito en ella, se estima que la cifra real debe ser mayor.

El mayor crecimiento se dio a partir de noviembre y diciembre de 2013:

Un asunto que tiñe la aceptación de *Bitcoin* es la practicidad, sobre todo a nivel tiempo. ¿Cuánto hay que esperar hasta que el bloque específico que contiene una transacción sea incorporado a la cadena de bloques? Para montos pequeños, la transacción se toma cómo válida apenas es notificada a la red. Para montos mayores, se recomienda esperar a que se sumen seis confirmaciones, o sea, una hora. En definitiva, cada comerciante podría establecer el umbral con el que se encuentre cómodo y, desde ya, se estudian maneras de acelerar el proceso sin crear vulnerabili-

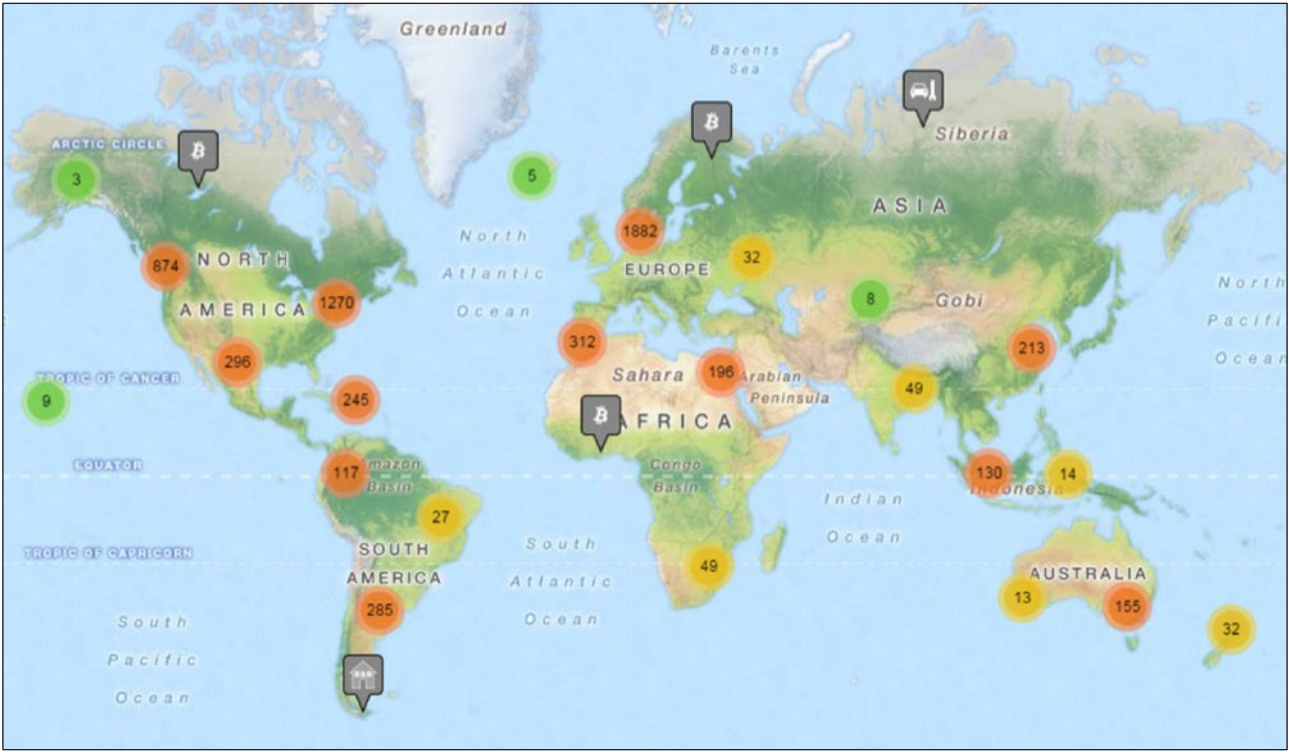
[41] MATONIS, JON. *Why Bitcoin Fungibility is Essential*, en Coindesk, 1 de diciembre de 2013. Acceso online: <http://www.coindesk.com/bitcoin-fungibility-essential/>; WYATT, CHANDLER. *Bitcoin Mixing Aims to Preserve Fungibility and Privacy*, en Coin.Consultancy, 10 de diciembre de 2013. Acceso online: <http://coinconsultancy.com/2013/12/10/bitcoin-mixing-aims-to-preserve-fungibility-and-privacy/>.

[42] DAVIDSON, JACOB. *No, Big Companies Aren't Really Accepting Bitcoin*, en Time, 9 de enero de 2015. Acceso online: <http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/>.

MAPA 1

Comercios que aceptan Bitcoin

Febrero 2015⁴³

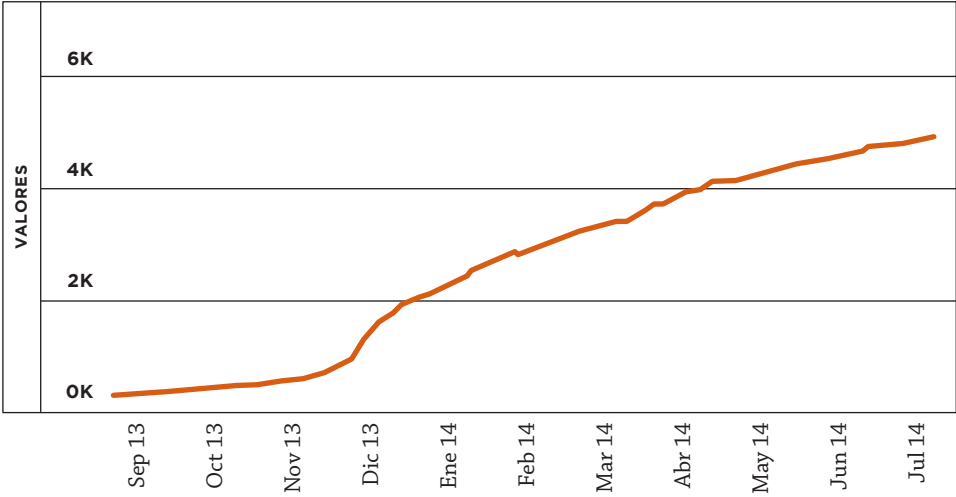


Fuente: Coinmap. © Colaboradores de OpenStreetMap.

GRÁFICO 6

Evolución de la aceptación de Bitcoin en comercios

Septiembre 2013 a Julio 2014⁴⁴



Fuente: Bitcoinpulse.

[43] Coinmap. Acceso online: www.coinmap.org © Colaboradores de OpenStreetMap.

[44] Bitcoinpulse. Acceso online: http://www.bitcoinpulse.com/chart/coinmap/num_venues/total.

dades ante potenciales atacantes⁴⁵. Más allá de estos recaudos, y pese a la mayor adopción de *Bitcoin* que se viene observando, nada asegura que tenga aceptación generalizada en el futuro. En este sentido, *Bitcoin* ha sido llamado *una solución en busca de un problema*.

3.1.2 Unidad de cuenta

La segunda función del dinero es la de ser unidad de cuenta. Debe poder usarse como numerario o referencia para fijar el precio de bienes y servicios muy disímiles entre sí. Al ser la medida del valor, simplifica el sistema de precios relativos y reduce los costos de información. La volatilidad de *Bitcoin* ha impedido que se consolide como unidad de cuenta y como

unidad de denominación de los contratos. Desde que comenzó a funcionar en 2009, la cotización de *Bitcoin* sufrió enormes fluctuaciones, sobre todo a partir de 2013, como se puede ver en el *Gráfico 7*.

El *Gráfico 8* hace foco en el período 2013-2015.

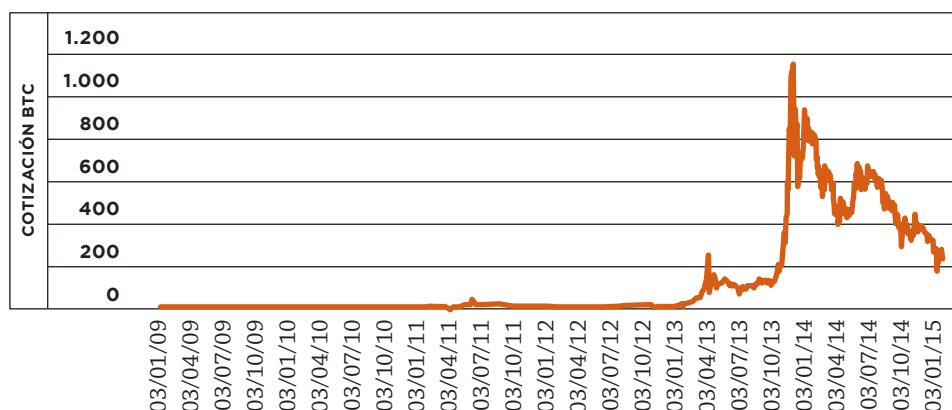
[45] ROSENFELD, MENI. *Analysis of hashrate-based double-spending*, en Bitcoil. Acceso online: <https://bitcoil.co.il/Doublespend.pdf> 20 de marzo de 2014; SOMPOLINSKY, YONATAN y ZOHAR, AVIV. *Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, not Chains*, Cryptology ePrint Archive. Acceso online: <http://eprint.iacr.org/2013/881.pdf>.

[46] Blockchain.info. Datos al 31 de enero de 2015.

[47] Ibidem.

GRÁFICO 7

Cotización de *Bitcoin* contra el USD 2009-2015⁴⁶



Fuente: Elaboración propia en base a Blockchain.info

GRÁFICO 8

Cotización de *Bitcoin* contra el USD 2013-2015⁴⁷



Fuente: Elaboración propia en base a Blockchain.info

El economista David Yermack calculó que entre el 01 de enero de 2013 y el 29 de noviembre de 2013, la volatilidad diaria anualizada del tipo de cambio BTC-USD fue del 133%. A efectos comparativos, la volatilidad del EUR, YEN, GBP y CHF en ese período fue del 8%-12%, la del oro del 22% y la de las acciones más transadas del 20%-30%. En cuanto a las acciones más riesgosas, *pocas veces exhiben volatilidades tan altas como el 100%*, observó Yermack. Además, el precio del BTC contra el USD no mostró correlación alguna con los precios de otras monedas ni con el precio del oro. Esto dificulta enormemente su uso como herramienta de manejo de riesgos y obstaculiza la protección efectiva contra los riesgos que afectan al propio Bitcoin⁴⁸.

[48] YERMACK, DAVID. *Is Bitcoin a real currency?*, NBER Working Paper Series, Working Paper 19747, 1 de diciembre de 2013. Pág. 7. Acceso online: <http://www.nber.org/papers/w19747>.

[49] Ver: IWAMURA, MITSURU et. al. *Can we stabilize the price of a Cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with Central Bank money*, Universidad de Hitotsubashi, 25 de octubre de 2014. Acceso online: <http://es.scribd.com/doc/245827939/SSRN-id2519367-Japan-Improved-Bitcoin-IBC>.

[50] Ibídem. Pág. 13.

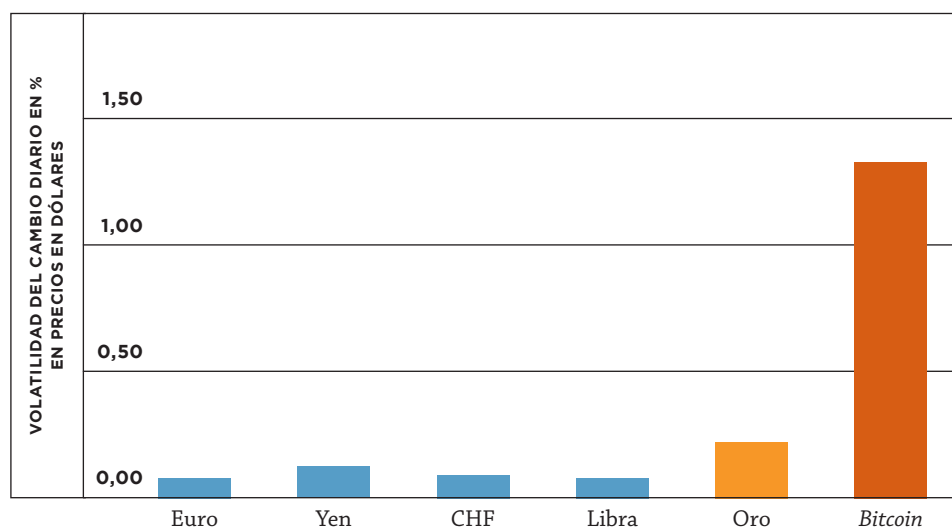
¿De qué depende el precio de *Bitcoin*? La oferta está determinada por el protocolo, por lo que siempre es conocida. En contraste, la demanda es muy difícil de predecir ya que no sólo depende de la demanda específica de *bitcoins* para transacciones, sino de otros factores tales como inconvenientes o fraudes perpetrados con *Bitcoin*, o acontecimientos no relacionados con los fundamentals de *Bitcoin* pero que afecten los ánimos de los mercados, como pueden ser una crisis bancaria o episodio de contagio financiero (por ejemplo, el caso de Chipre en 2013).

Los defensores de *Bitcoin* dicen que la volatilidad se debe a la novedad del fenómeno, al tamaño relativamente pequeño del mercado, a la incertidumbre que genera la tecnología en muchos sectores sociales y a la incógnita sobre su evolución futura. Argumentan, por lo tanto, que a medida que se expanda y consolide *Bitcoin*, la volatilidad de su precio se reducirá, formando así un círculo virtuoso. Una visión menos optimista subraya que la volatilidad es inherente a *Bitcoin*⁴⁹.

GRÁFICO 8

Volatilidad de *Bitcoin* contra otras monedas y oro

Enero-Noviembre 2013⁵⁰



Fuente: Yermack, David.

3.1.3 Reserva de valor

La tercera función del dinero, realizada por Keynes en sus críticas a la teoría clásica, es la de reserva de valor: debe conservar su valor a través del tiempo para garantizar la compra de bienes y servicios en el futuro⁵¹. Aunque el dinero no es la única reserva de valor en la economía, sí es la más líquida.

La durabilidad, entonces, es un requisito esencial y *Bitcoin* lo cumple con creces. Su naturaleza digital impide la degradación física por el paso del tiempo o por algún acontecimiento indeseado (incendio, inundación, etc.). Tampoco tiene problemas de escala para ser guardado. Aunque la cadena de bloques se volverá más larga y pesada, sólo se requieren ajustes técnicos para facilitar su almacenamiento.

Otra propiedad importante es que el dinero debe conservar un valor relativamente estable. Como se vio en el apartado anterior, hasta ahora la enorme volatilidad de *Bitcoin* en un período tan corto hace que sea inadecuado como reserva de valor. Mantener *Bitcoin*, incluso por poco tiempo, es una propuesta de alto riesgo y su volatilidad genera gran incertidumbre.

Más allá de las cotizaciones coyunturales, hay que tener en cuenta cuestiones estructurales, en particular, el hecho de que la oferta máxima de *bitcoins* está fijada en 21 millones de unidades. Por un lado, esto evita que se produzca una espiral inflacionaria como podría suceder con una creación de dinero mayor a la deseada por parte de los Bancos Centrales. Quienes apoyan a *Bitcoin* señalan que, en este sentido, el dinero fiduciario no se caracteriza justamente por ser una gran reserva de valor y que *Bitcoin* se encuentra blindada contra esta clase de manipulaciones.

Por otro lado, paradójicamente, esta característica podría generar deflación. Suponiendo que *Bitcoin* llegara a un amplio nivel de aceptación, con la oferta fija y una demanda creciente, su valor seguiría subiendo, mientras que los precios de los bienes y servicios irían bajando. En este escenario, las personas acapararían sus *bitcoins* ya que éstos tendrían una capacidad de compra cada vez mayor. Sin embargo, las empresas se verían imposibilitadas de concretar una ganancia porque los precios de sus productos serían cada vez más bajos, los deudores se verían seriamente perjudicados porque el valor de sus deudas en *bitcoins* sería cada vez más alto y, como resultado, la actividad económica y la confianza se verían dañadas (efecto Fisher)⁵². En este contexto, los *bitcoins* se valorizarían respecto de otros bienes y servicios pero, como nadie quisiera gastarlos, serían un pobre medio de intercambio. Aquí se genera el problema: si ya no fuera tomado como medio de intercambio, entonces no tendría utilidad como moneda, y su valor caería a cero. Varios estudios apuntan a que la gente prefiere guardar sus *bitcoins* antes que gastarlos, y la proporción que todavía no ha sido gastada supera el 60%⁵³. Este hecho constituye una preocupación legítima pero no un resultado predestinado ya que, aunque se conoce la oferta futura de *bitcoins*, la demanda es una incógnita. Si la moneda lograra consolidarse como medio de intercambio útil y generalizado, quizás ayudaría a evitar el *Dilema del Acaparador*.

[51] KEYNES, JOHN MAYNARD. *Teoría General de la ocupación, el interés y el dinero*. México: Fondo de Cultura Económica, 1995, 2° Ed.

[52] FISHER, IRVING. *The Debt-Deflation Theory of Great Depressions*, en *Econometrica*, Vol. 1, N°4, 1933; Hamada. Ver también: KOICHI; KASHYAP, ANIL K. y WEINSTEIN, DAVID E. *Japan's Bubble, Deflation and Long-term Stagnation*. Cambridge, Mass: MIT Press, 2011.

[53] MEIKLEJOHN, SARAH, et. al. *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, en UCSD CSE Web, Octubre de 2013. Acceso online: <http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>. Ver también: RON, DORIT y ADI, SHAMIR. *Quantitative Analysis of the Full Bitcoin Transaction Graph*, The Weizmann Institute of Science, Israel. Acceso online: <https://eprint.iacr.org/2012/584.pdf>.

La pregunta sobre el valor de *Bitcoin* y su sello deflacionario implícito generan todo tipo de interrogantes. Algunos son:

TABLA 7
Algunos interrogantes

Bitcoin y el patrón oro	Dada la oferta limitada de <i>bitcoins</i> , y dado que el sistema fue diseñado para reproducir el ritmo de minería del oro, ¿cuáles son las similitudes y diferencias del sistema <i>Bitcoin</i> con el patrón oro?
	¿Sufrirá las mismas ventajas (falta de inflación) y desventajas (deflación, límites al crecimiento económico, amplificación de los shocks económicos negativos, perjuicios a los deudores) que el patrón oro? ⁵⁴
Reglas vs. Discreción	Otra arista que surge a partir de este diseño es el clásico debate de <i>Reglas vs. Discreción</i> ⁵⁵ .
	El hecho de que el ritmo de emisión de <i>Bitcoin</i> esté sujeto a una regla conocida de antemano ayuda a reducir la incertidumbre. No obstante, también reduce la flexibilidad y margen de actuación ante los diversos <i>shocks</i> económicos.
	Incluso si se piensa que es mejor operar con una regla, no es seguro que <i>Bitcoin</i> ofrezca la mejor. Cabe mencionar que el propio Milton Friedman, que no era ningún simpatizante de la Reserva Federal, propuso encargarle a una computadora la tarea de emitir dinero con un ritmo de crecimiento prefijado –mayor a cero– del $k\%$ anual ⁵⁶ .
	El hecho de que no se pueda aplicar un <i>target</i> de inflación con <i>Bitcoin</i> impide su uso como ancla nominal de precios.
Valor subyacente de Bitcoin	El valor subyacente del oro radica en su escasez y en sus propiedades físico-químicas que lo vuelven durable y poco susceptible a adulteraciones. Se utiliza en procesos industriales y en la joyería.
	El valor subyacente del dinero fiduciario es que el Estado la declara de curso legal forzoso, por lo que debe ser aceptado obligatoriamente para el pago de impuestos, deudas, salarios, etc. Detrás de este arreglo se encuentra tácito lo que Max Weber denomina el monopolio de la violencia del Estado.
	<i>Bitcoin</i> no cumple con las características del oro (salvo la escasez) ni es de curso legal, y esto es justamente la ideología implícita en su diseño.
	¿Cuál es, entonces, el valor subyacente de <i>Bitcoin</i> ? Para algunos es el protocolo mismo, el poder de la criptografía. Para otros, no tiene valor subyacente, y algunos van más allá y dicen que no necesariamente debería tener uno. Con tal de que las personas le asignen un valor, puede funcionar, y esta dosis de consenso colectivo no se diferencia de las creencias sociales que se ponen en juego en torno al dinero fiduciario.

[54] Ver: EICHENGREEN, BARRY. *Golden Fetters: The Gold Standard and the Great Depression, 1919-1939*. Nueva York: Oxford University Press, 1992; BAYOUMI, TAMIM A; EICHENGREEN, BARRY y TAYLOR MARK P. *Modern perspectives on the gold standard*. Nueva York: Cambridge University Press, 1996.

[55] Ver, por ejemplo: KYDLAND, FINN E. y PRESCOTT, EDWARD. C. *Rules Rather than Discretion: The Inconsistency of Optimal Plans*, en *The Journal of Political Economy*, Vol. 85, N°3, junio de 1977. Pág. 473-492 Acceso online: http://www.tek.uni-corvinus.hu/files/szovegek/kydland_prescott_rules_rather_than_discretion.pdf; BARRO, ROBERT J. y GORDON, DAVID B. *Rules, Discretion and Reputation in a Model of Monetary Policy*, en *Journal of Monetary Economics*, N°12, Julio de 1983. Pág. 101-121. Acceso online: <http://www.wm.tu-berlin.de/fileadmin/fg124/geldtheorie/literatur/barro-gordon-c.pdf>.

[56] FRIEDMAN, MILTON. *The Optimum Quantity of Money*, en *The Optimum Quantity of Money and Other Essays*. Chicago: Aldine Publishing Company, 1969. Pág. 1-50.

3.2 Bitcoin como activo

Algunos dicen que *Bitcoin* en realidad no es dinero, sino un activo alrededor del cual se ha formado una poderosa burbuja especulativa. Algunas figuras del mundo económico que se han pronunciado en este sentido son Alan Greenspan, Warren Buffet y Robert Shiller⁵⁷.

A fin de 2013 dominaban las clásicas señales de *manía especulativa*, con precios que parecían no tener techo, optimismo desbordante y gran cobertura mediática. Abundaban las historias de personas que se habían vuelto fantásticamente ricas por haber comprado *bitcoins* y de personas que se habían perdido la oportunidad de sus vidas por no haberlo hecho⁵⁸.

La cotización de *Bitcoin* podría asemejarse a la de otras conocidas burbujas, como la Tulipomanía, la Burbuja de los Mares del Sur o la Crisis de las Puntocom.

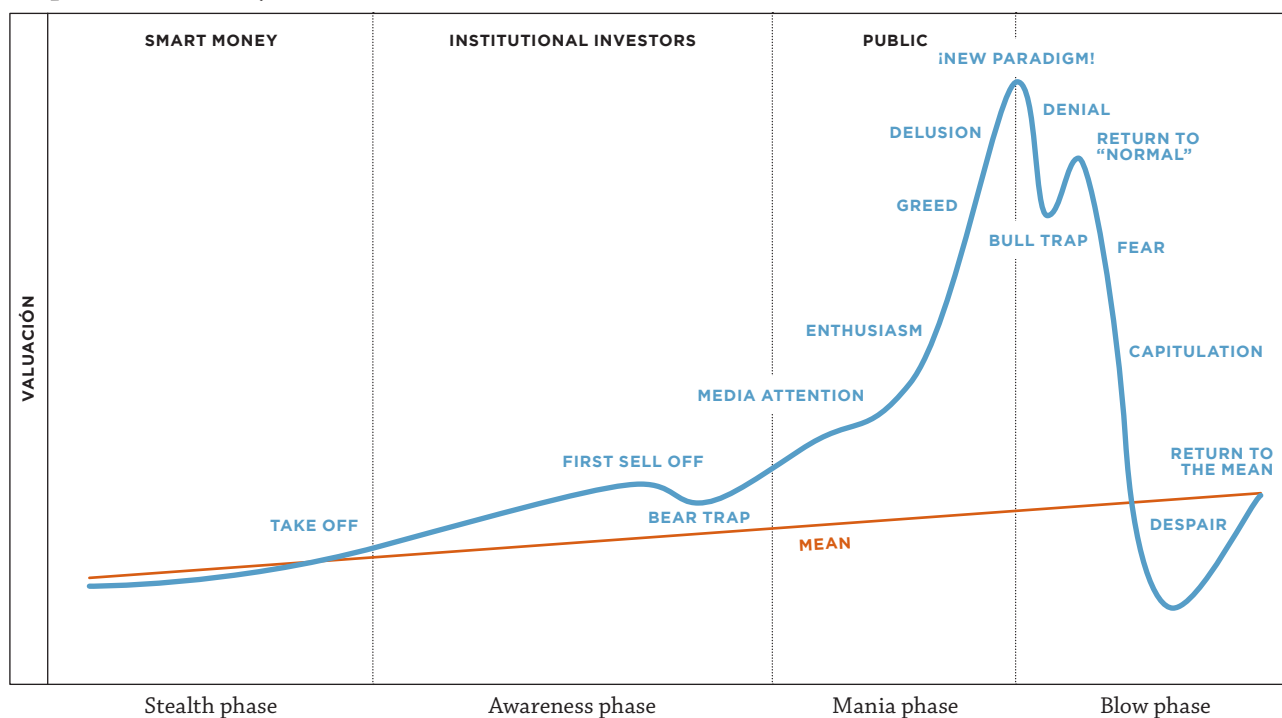
[57] CRIPPEN, ALEX. *Buffett blasts bitcoin as mirage: Stay away!*, en CNBC, 14 de marzo de 2014. Acceso online: <http://www.cnbc.com/id/101494937>; KEARNS, JEFF. *Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value*, en Bloomberg, 4 de diciembre de 2014. Acceso online: <http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.html>; WEISENTHAL, JOE. *Robert Shiller: Bitcoin Is An Amazing Example Of A Bubble*, en Business Insider, 24 de enero de 2014. Acceso online: <http://www.businessinsider.com/robert-shiller-bitcoin-2014-1>.

[58] Ver, por ejemplo: GIBBS, SAMUEL. *Man buys \$27 of bitcoin, forgets about them, finds they're now worth \$886k*, en The Guardian, 29 de octubre de 2013. Acceso online: <http://www.theguardian.com/technology/2013/oct/29/bitcoin-forgotten-currency-norway-oslo-home>.

[59] COLOMBO, JESSE. *Bitcoin May Be Following This Classic Bubble Stages Chart*, en Forbes, 19 de diciembre de 2013. Acceso online: <http://www.forbes.com/sites/jessecolombo/2013/12/19/bitcoin-may-be-following-this-classic-bubble-stages-chart/>. Imagen: *Stages of a bubble*, Jean-Paul Rodrigue, Universidad de Hofstra.

GRÁFICO 9

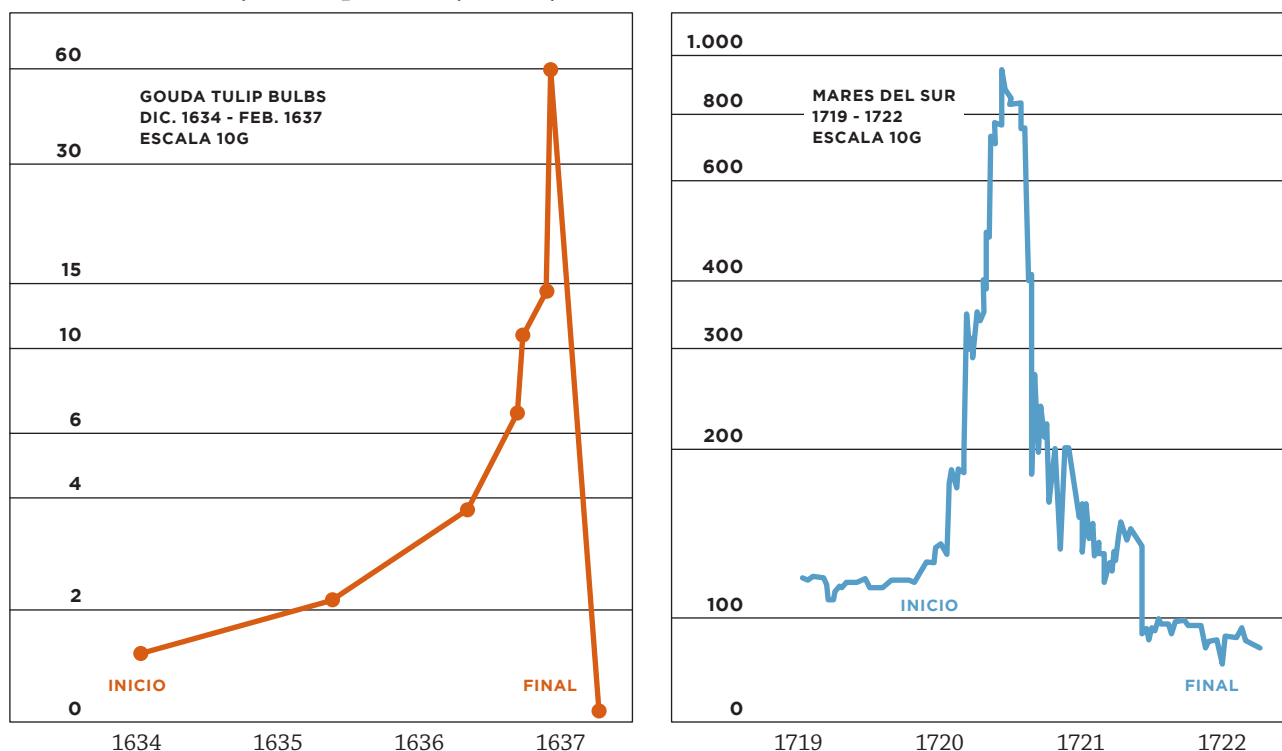
Etapas de una burbuja⁵⁹



Fuente: Jean-Paul Rodrigue, Universidad de Hofstra.

GRÁFICO 10

Dos famosas burbujas: Tulipomanía y Burbuja de los Mares del Sur⁶⁰



Fuente: Elliot Wave International.

Sin embargo, a diferencia de estas burbujas, que crecieron hasta pincharse, *Bitcoin* es sorprendentemente resistente. De hecho, hubo varias instancias que podrían catalogarse como burbujas –en 2011 pasó de USD 0,8 a USD 31 y luego a USD 16, en marzo y abril de 2013 pasó de USD 100 a USD 266, y luego a USD 50, y en octubre y noviembre de 2013 pasó de USD 130 a más de USD 1.000, y luego se redujo a USD 500– y ninguna ha marcado el fin de *Bitcoin*. Los defensores de *Bitcoin* creen que, en el fondo, el pinchamiento de las sucesivas burbujas es positivo para el sistema en su conjunto, porque deja a los *verdaderos creyentes* como participantes y, además, contribuye a solidificar la madurez de la comunidad.

[60] Elliot Wave International. Acceso online: www.elliottwave.com

[61] FRANKEL, TAMAR. *The Ponzi Scheme Puzzle. A History and Analysis of Con Artists and Victims*. Nueva York: Oxford University Press, 2012.

3.3 Bitcoin como Esquema Ponzi

Bitcoin ha sido denunciado como Esquema Ponzi, o sea, un esquema de inversión fraudulenta que promete ganancias seguras y mayores a las que pudieran obtener en el mercado. En estos sistemas, se genera un ciclo en el que se les paga a los inversores viejos con el dinero de los inversores nuevos, y no con las ganancias de algún negocio concreto. Estas estafas siempre sufren un colapso final a expensas de los últimos participantes. El nombre deriva de Carlo Ponzi, un inmigrante italiano a EEUU que, en 1920, perpetró un engaño de este tipo que les generó enormes pérdidas a las víctimas⁶¹.

Bitcoin no es un Esquema Ponzi porque no hay una autoridad centralizada u organizadora que diseña el sistema y, lo más importante, no hay ninguna promesa o garantía de obtener una ganancia⁶². Cada persona que compra *Bitcoin* lo hace a su propio riesgo, y la volatilidad de la cotización no es precisamente un secreto. Desde luego, esto no impide que ciertos estafadores organicen Esquemas Ponzi utilizando *Bitcoin*, aprovechándose del deseo de ganar dinero y de la relativa ignorancia de algunos inversores sobre el tema de las monedas virtuales⁶³.

La diferencia es clara. Entonces, ¿por qué hay quienes dicen que el propio sistema de *Bitcoin* es un Esquema Ponzi? Quizás la confusión tenga que ver con los beneficios de los primeros usuarios de *Bitcoin*:

- Los primeros mineros se beneficiaron más que los actuales porque, en un principio, cada bloque ofrecía 50 *bitcoins* como recompensa, cifra que se va reduciendo a la mitad cada cuatro años.
- Quienes compraron *bitcoins* en los primeros años a valor casi cero se vieron beneficiados por la enorme suba de precios, aún teniendo en cuenta el pinchamiento de las burbujas.

Sin embargo, podría argumentarse que, al igual que los primeros inversores en nuevas empresas, se trata de evaluar la relación entre riesgo y recompensa. Los primeros mineros y compradores de *Bitcoin* de algún modo asumieron más riesgos ante una posibilidad de inversión cargada de incertidumbre. Podría haberles ido bien o mal.

3.4 *Bitcoin* como facilitador de actividades ilegales

Por las características de *Bitcoin*, algunos aseguran que es una herramienta ideal para llevar adelante todo tipo de actividades ilegales: lavado de dinero, compra y venta de bienes y servicios ilegales (drogas, armas, juego, asesinatos por encargo y pornografía infantil), y financiamiento de actividades ilícitas (terrorismo y trata de personas).

El caso más importante que involucró a *Bitcoin* con el mundo de la criminalidad fue el de Silk Road, una página conocida como *el Amazon de las drogas*. Allí se podía comprar y vender todo tipo de sustancias, siempre usando *bitcoins* como medio de pago. La página, que formaba parte de la *web profunda*, fue lanzada en febrero de 2011 y cerrada por el FBI en octubre de 2013, aunque después hubo un relanzamiento (con otros operadores) y diversos imitadores⁶⁴. Se estima que, entre febrero de 2011 y julio de 2013, Silk Road tuvo un total de ventas por 9,5 millones de *bitcoins*, por las que cobró comisiones de 614.000 *bitcoins*⁶⁵. A partir de la clausura de la página, por un tiempo el gobierno estadounidense se convirtió en uno de los mayores tenedores de *bitcoins*. El FBI requisó unos 144.000 *bitcoins* del supuesto líder de Silk Road, Ross Ulbricht, y otros 30.000 *bitcoins* de Silk Road que fue-

[62] Un reciente estudio de Kaushik Basu, economista del Banco Mundial, afirma que *Bitcoin* es un Esquema de Ponzi natural, lo que significa que, en su visión, es una burbuja de activos. Ver: BASU, KAUSHIK. *Ponzis. The Science and Mystique of a Class of Financial Frauds*, Policy Research Working Paper WPS6967, Banco Mundial, Julio de 2014. Acceso online: http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2014/07/16/000112742_20140716115536/Rendered/PDF/WPS6967.pdf.

[63] SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme, en Securities and Exchange Commission. Acceso online: https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.UomLP_mSzHQ; *Ponzi Schemes Using Virtual Currencies*. Acceso online: http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf.

[64] SEGAL, DAVID. *Eagle. Scout. Idealist. Drug Trafficker?*, en The New York Times, 18 de enero de 2014. Acceso online: <http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html>; CHRISTIN, NICHOLAS. *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*, noviembre de 2012. Acceso online: <http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf>.

[65] *United States of America v. Ross William Ulbricht*. Pág. 15. Acceso online: <https://www.documentcloud.org/documents/801103-172770276-ulbricht-criminal-complaint.html>.

ron subastados a fin de junio de 2014⁶⁶. El ganador de la subasta, el capitalista de riesgo Tim Draper, afirmó que trabajaría junto a la *startup* Vaurum para llevar *Bitcoin* a los países emergentes: “Esperamos crear nuevos servicios que provean liquidez y confianza a mercados que han sido paralizados por monedas débiles”⁶⁷.

Durante el cierre de Silk Road, comentaristas se preguntaban si sería el fin de *Bitcoin*. Lo cierto es que, si bien hubo una reducción en el precio, logró sobrevivir a esta prueba. Según los defensores de la criptomoneda, el episodio fue positivo porque ayudó a sanear su imagen⁶⁸. En realidad, la expansión y consolidación de *Bitcoin*, con una estabilización de su valor, y el refinamiento de las técnicas de anonimato, proveería mayor incentivo para usarlo con fines ilícitos, por su facilidad para realizar transacciones internacionales. Sin embargo, por el momento, la moneda más usada para fines ilegales sigue siendo el dólar estadounidense, en efectivo.

Por otra parte, sería miope reducir a *Bitcoin* a una mera herramienta del crimen. Sin negar que se utilice para realizar actividades ilegales, conviene enmarcar este aspecto en una caracterización más amplia: la de *Bitcoin* como circuito alternativo de pagos que permite operar por fuera de los controles de gobiernos e instituciones financieras. Como mostró el *bloqueo financiero* a WikiLeaks en 2012 por parte de Visa, Mastercard, Paypal, Bank of America y Western Union, la capacidad que tiene *Bitcoin* de operar por fuera de los canales tradicionales no debe ser subestimada⁶⁹. Es así que se vuelve deseable por motivos ideológicos, por conveniencia o para eludir normativas perjudiciales.

Hay quienes se ven atraídos hacia *Bitcoin* por motivos ideológicos. Los usuarios de *Bitcoin* tienen todo tipo de pensamientos políticos, pero la criptomoneda tiene especial popularidad entre los libertarios. Éstos se entusiasman con el relativo anonimato de las transacciones, la posibilidad de generar una alternativa al dólar estadounidense y la posibilidad de quitarles poder a los gobiernos y Bancos Centrales. Por lo general, en el plano económico, se basan en las ideas de la Escuela Austríaca⁷⁰.

El motivo de la conveniencia también tiene peso propio. Tal como identificó un informe de Citi, *Bitcoin* tiene una sustancial ventaja en términos de costos de transacción sobre tradicionales intermediarios financieros que procesan transferencias electrónicas de efectivo y que operan tarjetas de débito y crédito. Para las empresas, el costo de aceptar *Bitcoin* es más bajo que la de aceptar tarjetas emitidas por bancos ya que éstas implican comisiones y costos por posibles fraudes. Para los consumidores, *Bitcoin* ofrece ventajas para transacciones internacionales, envío de remesas, pagos por internet y micropagos. Es así que instituciones como Visa, Mastercard e incluso Paypal miran el fenómeno *Bitcoin* con cierto recelo⁷¹. “Visa y Mastercard deben estar sudando la gota gorda”, dijo Campbell R. Harvey, profesor de Finanzas en la

[66] *Silkroad Seized Coins*, en Blockchain.info. Acceso online: <https://blockchain.info/address/1F1tAaz5x1HUXrCNLbtMDqcw605GNn4xqX>; *DPR SeizedCoins*, en Blockchain.info. Acceso online: <https://blockchain.info/address/1FfmbHfnpaZjKFvyi10kTjJusN455paPH>.

[67] *Tim Draper Wins Gov't Auction, Partners With Vaurum to Provide Bitcoin Liquidity in Emerging Markets*, comunicado de Vaurum, en Medium, 2 de julio de 2014. Acceso online: <https://medium.com/@vaurum/tim-draper-wins-govt-auction-partners-with-vaurum-to-provide-bitcoin-liquidity-in-emerging-markets-88fo4a1d8598>; KHARIF, OLGA y DOUGHERTY, CARTER. *VC Tim Draper Wins Entire Cache in Bitcoin Auction*, en Bloomberg, 2 de julio de 2014. Acceso online: <http://www.bloomberg.com/news/2014-07-01/bitcoin-auction-ends-single-bidder-wins-entire-cache.html>.

[68] Ver, por ejemplo: EHA, BRIAN P. *Could the Silk Road closure be good for Bitcoin?*, en The New Yorker, 5 de octubre de 2014. Acceso online: <http://www.newyorker.com/online/blogs/currency/2013/10/could-the-silk-road-closure-be-good-for-bitcoin.html>.

[69] MATONIS, JON. *WikiLeaks Bypasses Financial Blockade With Bitcoin*, en Forbes, 20 de agosto de 2012. Acceso online: <http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/>.

[70] Ver, por ejemplo: VON HAYEK, FRIEDRICH. *Denationalization of money: the argument refined*. Londres: Institute of Economic Affairs, 1978.

[71] *Disruptive Innovations II*, Citi GPS, mayo de 2014. Acceso online: <https://ir.citi.com/9rwxD8AaCyk42k1RUTFT2tBTUAcB8W%2F8ol1Q8pQCeeldnPGx6BkFuTAGInt15pi6Ws6bMZieRM%3D>.

Universidad de Duke. “*Estamos en el ocaso de la comisión del 2%-3% del duopolio [...] Es demasiado temprano para decir si el modelo de Bitcoin será el ganador. Pero es obvio que vamos hacia una nueva era con comisiones de transacciones mínimas*”⁷². Es evidente que las instituciones financieras ejercerán su ingenio y capacidad de lobby para aprovechar el fenómeno *Bitcoin* a su favor (por ejemplo, emitir tarjetas de crédito basadas en cuentas de *Bitcoin*) o, al menos, minimizar los daños (por ejemplo, declarando a las empresas que aceptan *Bitcoin* como de alto riesgo). Según Roman Leal, analista de Servicios de IT de Goldman Sachs, hay que ver además si *Bitcoin* logra mantener su ventaja de costo. “*Es probable que la creciente regulación incremente el costo de manejar Bitcoin, y quizás los proveedores de Bitcoin se vean obligados a transferirles este costo a los consumidores mediante mayores comisiones. También es probable que aumenten los costos operativos a medida que crezcan las operaciones. Al mismo tiempo, es probable que los procesadores de pagos tradicionales respondan reduciendo sus márgenes de ganancias y cooptando la tecnología y/o realizando otros cambios estructurales para mantenerse competitivos*”⁷³.

Otro atractivo es que, con *Bitcoin*, se podría eludir a los gobiernos, esquivando leyes impositivas o normas que regulan el flujo de capitales a través de las fronteras. Evitar los controles de capital es un claro ejemplo⁷⁴. Es más, dos de los episodios de alza de valor de *Bitcoin* en 2013 tuvieron que ver con la elusión de ciudadanos de controles de capital: el corralito impuesto en Chipre y el crecimiento de la demanda en China.

La virtud de *Bitcoin* como circuito alternativo se topa con la pregunta del anonimato. ¿Qué tan anónimo es? Aquí, hay que considerar varios factores. El sistema pseudónimo (publicidad de las transacciones/ ocultamiento de las identidades) hace teóricamente imposible ligar las direcciones con sus dueños, pero existen técnicas para rastrear patrones y tendencias en las transacciones⁷⁵. Sumado a esto, la propia comunidad *Bitcoin* puede interesarse en monitorear las transacciones de alguna billetera considerada sospechosa, en una suerte de *vigilantismo* que impone la

moral de la propia comunidad. Pese a esto, las técnicas de protección del anonimato evolucionan día a día, tal como se evidencia con los servicios de *lavandería* que, a cambio de una pequeña comisión, mezclan los *bitcoins* provenientes de distintas direcciones para imposibilitar su asociación al verdadero origen. Además, hay algunas criptomonedas que buscan avanzar sobre *Bitcoin* en temas de privacidad, como *Zerocoin*⁷⁶.

Por eso, los reguladores y agentes judiciales suelen concentrar sus esfuerzos en las fronteras del mundo *Bitcoin*, aquellos lugares de entrada y salida, donde hay vínculos más sólidos con las identidades reales de los usuarios (por ejemplo, cuentas bancarias)⁷⁷. Esto se vio en el caso de Sheep Marketplace, un imitador de Silk Road que operó un defalco a sus usuarios⁷⁸. Los dueños de las direcciones sospechadas se vieron atrapados en una situación paradójica: tener muchos *bitcoins* pero no poder realizar transacciones con ellos.

[72] *Is Bitcoin a Bubble? Analysis from Professor Campbell Harvey*, 21 de enero de 2014. Acceso online: http://www.fuqua.duke.edu/news_events/news-releases/harvey-bitcoin-analysis/#.U59D5ZR5N1Y.

[73] LEAL, ROMAN. *Is Bitcoin the future of payments?*, en Global Macro Research, Top of Mind, N° 21, 11 de marzo de 2014. Pág. 18.

[74] WORSTALL, TIM. *Finally, A Proper Use for Bitcoin, Avoiding Capital Controls*, en Forbes, 21 de noviembre de 2013. Acceso online: <http://www.forbes.com/sites/timworstall/2013/11/21/finally-a-proper-use-for-bitcoin-avoiding-capital-controls/>.

[75] Ver: REID, FERGAL y HARRIGAN, MARTIN. *An Analysis of Anonymity in the Bitcoin System*, Julio de 2011. Acceso online: http://arxiv.org/pdf/1107.4524.pdf?origin=publication_detail; ANDROULAKI, ELLI ET AL. *Evaluating User Privacy in Bitcoin*. Acceso online: <http://eprint.iacr.org/2012/596.pdf>; MOSER, MALTE ET AL. *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, 2013. Acceso online: <http://maltemoeser.de/paper/money-laundering.pdf>; Meiklejohn, Sarah, et. al. Op. Cit.; Ron, Dorit y Adi, Shamir. Op. Cit.

[76] Zerocoin Project. Acceso online: <http://zerocoin.org/>.

[77] *Bitcoin Virtual Currency: Intelligence Unique Features Present. Distinct Challenges for Deterring Illicit Activity*, 24 de abril de 2012. Acceso online: <http://cryptome.org/2012/05/fbi-bitcoin.pdf>.

[78] KAMINSKA, IZABELLA. *Capital controls, Bitcoin edition*. Acceso online: <http://ftalphaville.ft.com/2013/12/04/1713032/capital-controls-bitcoin-edition/>.

En cierto modo, la descripción de *Bitcoin* como circuito alternativo podría relacionarse al concepto de Michel Foucault de heterotopía (del griego, *Hetero*=otro; *Topos*=lugar). Por este término, se entiende un espacio de otredad que funciona en condiciones no hegemónicas, y que representa, impugna, invierte o desenmascara las relaciones de poder implícitas en las tramas sociales. Es un *espacio fuera de todos los espacios* donde las funciones y las percepciones se desvían en relación con los lugares comunes donde la vida humana se desarrolla⁷⁹. El aspecto virtual de *Bitcoin*, su falta de localización geográfica y la forma en que expone las relaciones económicas y sociales en el uso de dinero, los sistemas de pagos y los contratos, lo vuelven una suerte de heterotopía.

3.5 Es el protocolo, estúpido

Quizás la faceta menos señalada –y más importante– de *Bitcoin* sea la de protocolo. Recordemos que *Bitcoin* es un protocolo de código abierto, es decir, su código fuente es de libre disponibilidad. Por lo tanto, puede ser usado de forma gratuita y también, si se quisiera, ampliado, modificado y redistribuido. También se podría utilizar la tecnología subyacente del *Blockchain* para crear nuevas aplicaciones, muchas de ellas con consecuencias formidables y disruptivas. Hay gran cantidad de empresas, *startups* e inversores trabajando en proyectos de todo tipo.

Una posible aplicación de *Bitcoin* son los **contratos inteligentes**. Éstos son protocolos que facilitan, verifican, monitorean, ejecutan o aplican el cumplimiento de determinadas cláusulas sin pasar por un intermediario, activando o desactivándose cuando se cumplen determinadas condiciones preestablecidas. En este sentido, podrían repensarse todos los sistemas de contratos que requieren de intermediarios y/o sistemas de validación (abogados, escribanos, registros públicos). Como afirmó Santiago Siri, emprendedor argentino y uno de los fundadores del Partido de la Red, el protocolo de *Bitcoin* podría considerarse *ley sin territorio* que tiene la capacidad de crear una *nueva burocracia*⁸⁰. Ejemplos de contratos inteligentes incluyen contratos financieros, agropecuarios, inmobiliarios, de apuestas

y cualquier contrato de transferencia de propiedad. También se podrían crear contratos en los que las decisiones se tomen o se realicen determinadas acciones cuando todos los socios den su autorización mediante sus firmas digitales, por ejemplo, la ejecución de un testamento⁸¹.

El proyecto Ethereum, por ejemplo, tiene como objetivo crear una nueva criptomoneda que tiene inscrita en su sistema la posibilidad de crear contratos inteligentes⁸². Otra experiencia interesante es ColoredCoins, un protocolo de código abierto que opera sobre el de *Bitcoin*. A nivel general, ColoredCoins son *bitcoins* que han sido *coloreados* por un atributo particular con el objetivo de diferenciarlos del resto, creando una nueva capa de información sobre los *bitcoins* subyacentes (como se ha dicho, esto quiebra la propiedad de fungibilidad). Se pueden usar los ColoredCoins para que las personas e instituciones puedan usar e intercambiar no sólo *bitcoins* sino también otros activos. Una alternativa es vincular *bitcoins* determinados con activos del mundo real (inmobiliarios, financieros, etc.). Otra opción es la emisión de un nuevo tipo de activo, como bonos, acciones, dinero privado (por ejemplo, puntos, cupones o millas en compañías aéreas)⁸³.

[79] FOUCAULT, MICHEL. *Des espaces autres*, conferencia en el Centre d'Études Architecturales, 14 de marzo de 1967. Publicado en *Architecture, Mouvement, Continuité*, N° 5, 1984. Pág. 46-49. Acceso online: <http://foucault.info/documents/heterotopia/foucault.heterotopia.en.html>.

[80] SIRI, SANTIAGO. Entrevista, 14 abril de 2014.

[81] Ver: SZABO, NICK. *Smart Contracts*, 1994. Acceso online: <http://szabo.best.vwh.net/smart.contracts.html>; SWANSON, TIM. *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management*. Amazon Digital Services, 2014. Acceso online: <https://s3-us-west-2.amazonaws.com/chainbook/Great+Chain+of+Numbers+A+Guide+to+Smart+Contracts%2C+Smart+Property+and+Trustless+Asset+Management+--+Tim+Swanson.pdf>.

[82] BUTERIN, VITALIK. *Ethereum White Paper. A Next Generation Smart Contract and Decentralized Application Platform*. Acceso online: <https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf>.

[83] *What are Colored Coins?*, en Colored Coins. Acceso online: <http://coloredcoins.org/about/what-are-coloredcoins/>.

Llevando los contratos inteligentes a un extremo, el protocolo de *Bitcoin* podría alterar radicalmente la naturaleza de las empresas, facilitando el paso desde las estructuras corporativas tradicionales a las **Corporaciones Autónomas Descentralizadas (CAD)** pensadas como contratos inteligentes de largo plazo. Las CAD son entidades autónomas que funcionan de forma descentralizada bajo un conjunto de reglas conocidas, generalmente protocolos de código abierto, que además son inmodificables salvo por consenso. Sus características son: corporaciones, autónomas, distribuidas, transparentes, confidenciales, confiables, fiduciarias (llevan a cabo la voluntad de sus clientes y *shareholders*), autorreguladas, incorruptibles y soberanas⁸⁴. *Bitcoin* podría pensarse como una CAD ya que funciona en base a un protocolo de código abierto, sin una autoridad central, aprovechándose de los servicios de los mineros y recompensándolos con *bitcoins*. La tecnología de la cadena de bloques podría utilizarse para sustentar otro tipo de CAD⁸⁵. Un clásico ejemplo es un auto sin conductor que los usuarios pagarían con *bitcoins*. En general, las CAD podrían utilizarse para realizar trabajos que nadie está dispuesto a hacer (sea por peligro, costo, ilegalidad, etc.) o trabajos para los que ofrecen beneficios singulares (menor costo, mayor velocidad, etc.). Las CAD llevarían a enormes cambios en los modos de entender la personería física y jurídica, en los tipos de sujetos y sus responsabilidades ante la ley, y también en la forma de operar de algunas industrias, por ejemplo, la de seguros. Generarían también transformaciones en el mundo del trabajo, desde el modo de concebir las empresas hasta el impacto directo sobre el empleo.

El protocolo de *Bitcoin* también podría servir como base de **mercados y servicios descentralizados**, tales como mercados de bonos, acciones y derivados. *Ripple* es un ejemplo de un servicio descentralizado que permite realizar transacciones con monedas virtuales, monedas fiduciarias (dólares, euros, yen), *commodities* y otras unidades (minutos de celular, puntos de comercios)⁸⁶. Algunos creen que esto sólo volvería aún más complejo el sistema financiero, alejándolo de la comprensión del común de la gente, mientras que otros creen que ayudaría a disminuir el poder de las instituciones con

importancia sistémica, reducir los márgenes de los intermediarios que cobran comisiones, facilitar las remesas internacionales y crear todo un mercado de micropagos, lo que, en definitiva, ayudaría a sanear el sistema. Otras aplicaciones interesantes son mercados descentralizados de predicciones, casinos *peer-to-peer* y servicios de mensajería descentralizados.

Otras posibilidades tienen que ver con los asuntos relacionados a la identidad. Para algunos analistas, uno de los errores clave de los creadores de Internet fue que no introdujeron un sistema confiable de identificación personal, lo que propició la aparición de redes sociales como Twitter y Facebook que gestionan las identidades virtuales de las personas pero accediendo a todos sus datos y almacenándolos en servidores centrales. Esto cambiaría si las redes sociales fueran descentralizadas ya que los usuarios lograrían mayor control de su información⁸⁷. También se podrían pensar en sistemas descentralizados de guardado de datos, registros descentralizados de propiedad intelectual, sistemas de reputación, y pensando más allá, se podrían reemplazar los actuales mecanismos de votación en las elecciones políticas, y crear diversos tipos de sistemas de votación para otros fines.

[84] LARIMER, STAN. *Bitcoin and the Three Laws of Robotics*, en *Let's Talk Bitcoin*, 14 de septiembre de 2013. Acceso online: <http://invictus-innovations.com/i-dac/>.

[85] BUTERIN, VITALIK. *Bootstrapping A Decentralized Autonomous Corporation: Part I*, en *Bitcoin Magazine*, 19 de septiembre de 2013. Acceso online: <http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/>; BUTERIN, VITALIK. *Bootstrapping An Autonomous Decentralized Corporation, Part 2: Interacting With the World*, en *Bitcoin Magazine*, 21 de septiembre de 2013. Acceso online: <http://bitcoinmagazine.com/7119/bootstrapping-an-autonomous-decentralized-corporation-part-2-interacting-with-the-world/>; BUTERIN, VITALIK. *Bootstrapping a Decentralized Autonomous Corporation, Part 3: IdentityCorp*, en *Bitcoin Magazine*, 24 de septiembre de 2013. Acceso online: <http://bitcoinmagazine.com/7235/bootstrapping-a-decentralized-autonomous-corporation-part-3-identity-corp/>.

[86] <https://ripple.com/>.

[87] ROSENBERG, SCOTT. *There's a blockchain for that!*, en Medium, 13 de enero de 2015. Acceso online: <https://medium.com/backchannel/how-bitcoins-blockchain-could-power-an-alternate-internet-bb501855af67>.

4. ¿MUERTE E IMPUESTOS?

4.1 Desafíos para la regulación

Es cierto que el protocolo de *Bitcoin* todavía está en su infancia pero, al contrario de lo que sucedía en los primeros días de Internet cuando pocos poseían una computadora, en la actualidad las personas tienen mucho mayor acceso a ellas y a los celulares, por lo que los cambios se producirían a una mayor velocidad. Así como el correo electrónico dejó casi obsoletos a las cartas, las postales y el fax, y así como Napster, Google, Facebook y Twitter revolucionaron la forma de interactuar con los contenidos, *Bitcoin* tiene un enorme potencial transformador social y económico.

A medida que *Bitcoin* iba ganando terreno, el fenómeno atrajo la atención de Bancos Centrales, gobiernos, agencias impositivas, supervisores bancarios, comisiones electorales, agencias de protección del consumidor, y agencias judiciales y policiales alrededor del mundo. Sus reacciones han sido variadas, desde estrategias de *wait-and-see* hasta prohibiciones lisas y llanas, pasando por investigaciones, advertencias, llamados a consultas públicas y elaboración de normas. Como dijo a fin de 2013 el Senador estadounidense, Thomas Carper, *las monedas virtuales, quizás más notablemente Bitcoin, han capturado la imaginación de algunos, generado miedo en otros, y confundido enormemente al resto*⁸⁸. Es así que el universo regulatorio de *Bitcoin* se encuentra en constante cambio.

Los desafíos que enfrentan los reguladores son múltiples. Las diversas facetas y funciones de *Bitcoin* hacen que sea un objeto elusivo difícil de definir. El enfoque elegido se convierte, pues, en la base de decisiones significativas, tales como si permitir o prohibir *Bitcoin*, si regularlo, si cobrar impuestos, y de qué maneras. Como resultado, cada agencia regulatoria lo aborda a través de sus anteojeas particulares y esto puede culminar en estrategias divergentes –y hasta contradictorias–, en una misma jurisdicción.

También es necesario seleccionar a los actores que serán sujetos de la regulación. Se le atribuye al ex Ministro de Relaciones Exteriores de EEUU Henry Kissinger la pregunta: “¿A quién llamo si quiero hablar con Europa?” De la misma manera, hoy los reguladores se encuentran desconcertados a la hora de *hablar con Bitcoin*. No hay nadie que emita *bitcoins*, nadie que controle el sistema y nadie a quien instar a realizar determinada acción u otra. No obstante, sí existen diversos actores involucra-

[88] Key Senate Committee Holds First Congressional Hearing on Virtual Currencies, US Senate Committee on Homeland Security and Governmental Affairs, 18 de noviembre de 2013. Acceso online: <http://www.hsgac.senate.gov/media/majority-media/key-senate-committee-holds-first-congressional-hearing-on-virtual-currencies>.

dos en el ecosistema de *Bitcoin*, tales como billeteras, sitios de intercambio (*exchanges*), servicios financieros, mineros, procesadores de pagos, emprendedores, desarrolladores, inversores, usuarios y comercios. Es en este ecosistema donde pueden realizarse esfuerzos regulatorios efectivos. Son los puntos de entrada y salida al sistema, las islas de centralización que persisten en el mar de descentralización. Esto no es tarea sencilla, pues cada actor tiene diferentes actividades, metas, riesgos, necesidades y preocupaciones.

Otro desafío que presenta *Bitcoin* es su naturaleza global. La red de usuarios y mineros no está localizada en ningún país específico y las transacciones traspasan fácilmente las fronteras nacionales. Sumado a eso, gran parte de las empresas del ecosistema *Bitcoin* dividen sus módulos de negocios en distintos países. Es así que las regulaciones nacionales no tienen la efectividad que quisieran los reguladores y, por el momento, tampoco se registran planes de cooperación internacional.

En este contexto, se plantea la pregunta de cuál sería la mejor estrategia regulatoria. Una posición es que el fenómeno es tan marginal que ni vale la pena regularlo. En su valor máximo de USD 1.151 la capitalización de mercado de *Bitcoin* fue de USD 13.900 millones, lo que podría asemejarse a la capitalización de una empresa grande. Hoy en día es de alrededor de USD 3 mil millones, similar a la de una empresa mediana⁸⁹. No tiene importancia sistémica y sus efectos sobre la economía global son limitados. Aún si no se fuera indiferente al fenómeno, podría pensarse que, como está cargado de tanta incertidumbre, conviene esperar a ver cómo evoluciona el ecosistema por sí mismo, sin el peso de una regulación inadecuada o miope, dándole espacio a la industria naciente para desarrollarse e innovar. Es más, muchas de las empresas del ecosistema *Bitcoin* adoptan por sí mismas estándares y mejores prácticas para autorregularse en cumplimiento de normas internacionales. Otra postura establece que es necesario regular *Bitcoin* de modo que, sin coartar la innovación, se logren minimizar los riesgos y generar confianza en el público, ayudando así a su

expansión. Una posición más extrema es considerar *Bitcoin* como instrumento peligroso y pasar a su prohibición.

4.2 Regulaciones de los distintos países

A nivel internacional, los gobiernos no han formulado una estrategia común o estándares uniformes para lidiar con *Bitcoin*. Sus reacciones han ido desde una observación despreocupada hasta la prohibición absoluta, pasando por advertencias al público y regulaciones específicas. Desde los organismos internacionales, tampoco ha habido una respuesta oficial contundente, salvo trabajos aislados de algunos economistas⁹⁰.

Hasta la fecha de elaboración de este trabajo (enero 2015), se han observado actitudes *hostiles* (rojo) por parte de Vietnam, Islandia, Bangladesh, Ecuador, Bolivia, y Kirguistán. En otros países, tales como China, India, Rusia, México, Colombia, Indonesia, Kazajistán, Jordania, Líbano y Taiwán, *Bitcoin* se encuentra en *disputa* (amarillo), con restricciones sobre su uso. El resto de los países, incluyendo EEUU, la UE, Reino Unido, Suiza, Brasil y la Argentina, han tenido actitudes *permisivas* (verde) o no han tomado determinación alguna sobre la criptomoneda.

4.2.4 Bitcoin en la Argentina

¿Cómo ha sido la recepción de *Bitcoin* por parte de las autoridades en la Argentina? Por ahora, sólo el Banco Central (BCRA) y Unidad de Información Financiera (UIF) hicieron declaraciones oficiales.

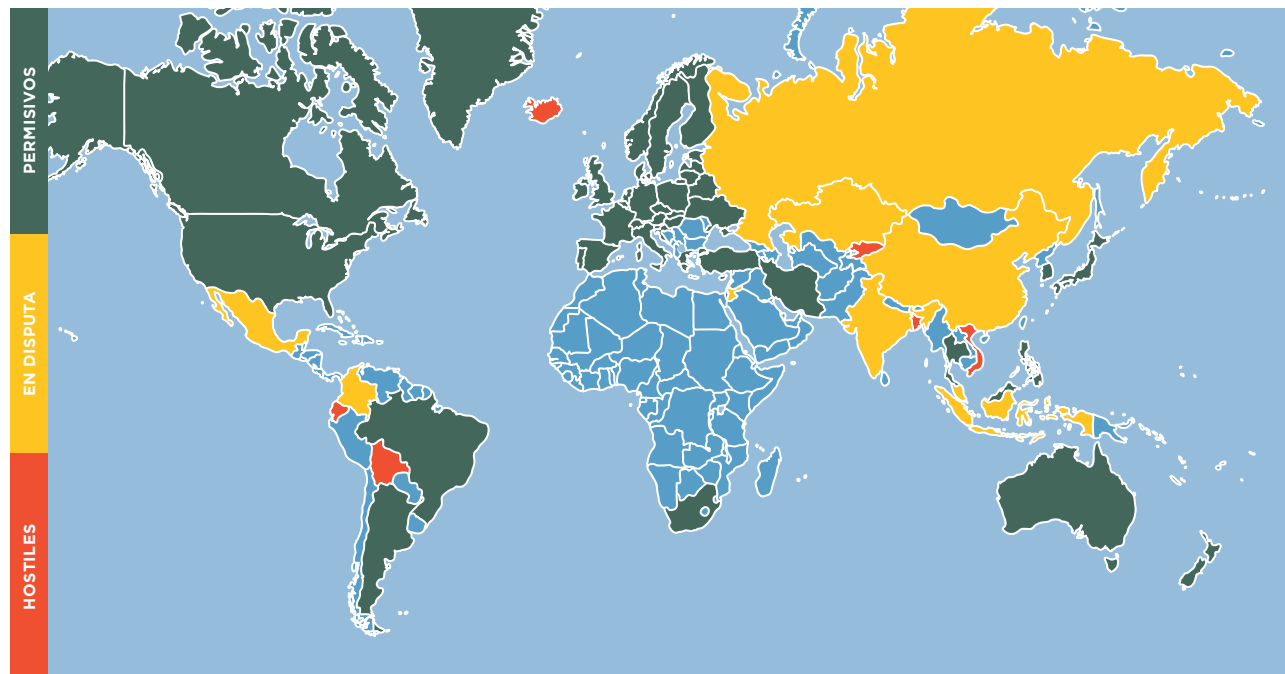
[89] Blockchain.info; *Market capitalization*, en Investopedia. Acceso online: <http://www.investopedia.com/terms/m/marketcapitalization.asp>

[90] Ver, por ejemplo: BLUNDELL-WIGNALL. *The Bitcoin Question. Currency versus Trust-less Transfer Technology*, OECD Working Papers on Finance, Insurance and Private Pensions, N°37, OECD, 16 de junio de 2014. Acceso online: <http://www.oecd-ilibrary.org/docserver/download/5jz2pwjd9t20.pdf?expires=1406231509&id=id&accname=guest&checksum=82B78Ao7B9D12CBEEC992D89126EFD97>.

MAPA 2

Mapa regulatorio de Bitcoin

Enero 2015



Fuente: Elaboración propia.

En mayo de 2014 el BCRA emitió un comunicado similar al de otros Bancos Centrales alrededor del mundo con el objetivo de *alertar al público en general* sobre los riesgos de operar con monedas virtuales. El BCRA señaló que las monedas virtuales *no son emitidas por este Banco Central ni por otras autoridades monetarias internacionales, por ende, no tienen curso legal ni poseen respaldo alguno*. El artículo 30 de la Carta Orgánica del BCRA dice:

“El Banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda. Se entenderá que son susceptibles de circular como moneda, cualesquiera fueran las condiciones y características de los instrumentos, cuando:

i) El emisor imponga o induzca en forma directa o indirecta, su aceptación forzosa para la cancelación de cualquier tipo de obligación; o

ii) Se emitan por valores nominales inferiores o iguales a 10 veces el valor del billete de moneda nacional de máxima nominación que se encuentre en circulación”⁹¹.

Por lo tanto, *Bitcoin* no entra en la definición del BCRA como moneda: no es emitido por una autoridad, su uso y aceptación es puramente opcional, y no mantiene una relación definida con la moneda nacional.

Otro aspecto de las monedas virtuales que resaltó el BCRA fue que *“no existen mecanismos gubernamentales que garanticen su valor oficial”*, por lo que están marcadas por la volatilidad de precio. También indicó que en el plano internacional *“aún no hay consenso sobre la naturaleza de estos activos”* y que *“diversas autoridades han advertido acerca de su eventual uso en operaciones de lavado de dinero y diversos tipos de fraude”*. Concluyó, por lo tanto, que los riesgos asociados a las monedas

[91] Carta Orgánica del BCRA, Ley 24.144. Pág. 16.
Acceso online: <http://www.bcra.gov.ar/pdfs/marco/ CartaOrganica2012.pdf>.

virtuales deben ser “soportados exclusivamente por sus usuarios”. De todos modos, el BCRA aclaró que “se encuentra actualmente analizando diversos escenarios para verificar que las operaciones con estos activos no se constituyan en un riesgo para aquellos aspectos cuya vigilancia está expresamente establecida en su Carta Orgánica”⁹².

Por su parte, en julio de 2014 la UIF emitió una resolución en la cual definió que los sujetos obligados por la Ley 25.246 (por ejemplo, entidades financieras, casas de cambio, agentes de bolsa, sociedades que exploten juegos de azar, empresas aseguradoras, corredores

inmobiliarios, etc.) a informar sobre posibles operaciones sospechosas de sus clientes “deberán prestar especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales y establecer un seguimiento reforzado respecto de estas operaciones evaluando que se ajusten al perfil del cliente que las realiza, de conformidad con la política de conocimiento del cliente que hayan implementado”. Para ello, a partir de agosto de

[92] Monedas virtuales. Comunicación al público en general. Banco Central de la República Argentina. Acceso online: www.bkra.gov.ar/bilmon/bmo23000.asp.

RECUADRO 1 Bitcoin y GAFI⁹³

En junio de 2014, el GAFI clasificó a Bitcoin como criptomoneda descentralizada y convertible:

Criptomoneda: “representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal en ninguna jurisdicción. No es emitida ni garantizada por ninguna jurisdicción, y cumple las funciones anteriores sólo por el acuerdo de la comunidad de usuarios de la moneda virtual”. Se diferencia del dinero fiduciario y del dinero electrónico que es la representación digital del dinero fiduciario.

Descentralizada: “distribuida, de código abierto, basado en la matemática, peer-to-peer”, es decir, “no tiene autoridad administrativa central, monitoreo central o control”.

Convertible: “tiene valor equivalente en dinero fiduciario y puede ser cambiada por dinero fiduciario”. En este sentido, se diferencia de monedas virtuales que son específicas a un dominio o mundo virtual, como Amazon.com o MMORPG (Massively Multiplayer Online Role-Playing Game), y que no pueden ser cambiados por dinero fiduciario.

El GAFI estableció que Bitcoin tiene usos legítimos, tales como la mejora de la eficiencia del sistema de pagos, la reducción de costos de transacción y la facilitación de micropagos y remesas internacionales. También identificó algunos riesgos potenciales. Bitcoin “ofrece un nivel de potencial anonimato imposible con tarjetas de crédito y débito o con sistemas de pago online más viejos como Paypal”, lo que eleva la posibilidad de lavado de dinero y financiación del terrorismo. Esto se exagera por el hecho de que se puede acceder al sistema desde cualquier parte del mundo. Sumado a eso, como los diversos servicios están segmentados, queda diluida la responsabilidad de supervisión y de cumplimiento de las normativas internacionales. Además, la velocidad de las transformaciones tecnológicas y de los modelos de negocios hace difícil el desarrollo de un armado regulatorio.

[93] Virtual Currencies. Key Definitions and Potential AML/CFT Risks, FATF Report, junio de 2014. Acceso online: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

2014 debían informar mensualmente sobre todas las operaciones que se realicen con monedas virtuales. De esta manera, las operaciones con *Bitcoin* recibirían el mismo tratamiento que el resto.

La UIF aclaró que, tal como especifica el Grupo de Acción Financiera Internacional (GAFI), entiende por *monedas virtuales* la “representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción”. Reconoció que, en los últimos tiempos, estas monedas han cobrado relevancia económica y que involucran una serie de riesgos para el sistema de prevención de los delitos de Lavado de Activos y de la Financiación del Terrorismo. Señaló como riesgos principales el anonimato que “impide la trazabilidad nominativa de las operaciones” y la facilidad para el “movimiento transfronterizo de activos, pudiendo participar de las mismas jurisdicciones que no tienen controles de prevención” del lavado de dinero y la financiación del terrorismo⁹⁴.

4.3. Competencia

Además de las regulaciones de los gobiernos, otro desafío que enfrenta *Bitcoin* es la competencia de cientos de criptomonedas. Muchas de ellas toman el protocolo *Bitcoin* –recordemos que es de código abierto– y cambian algún aspecto puntual, mientras que otras crean nuevos protocolos. Litecoin, por ejemplo, se basa en el protocolo de *Bitcoin* pero incorpora mayor velocidad en la creación de bloques –uno cada 2,5 minutos en vez de uno cada 10 minutos–, lo que permite procesar un mayor volumen de transacciones. Se llegarán a crear 84 millones de litecoins, 4 veces la cantidad total de bitcoins⁹⁵. Darkcoin también se basa en el protocolo de *Bitcoin* pero está modificado para producir un sistema anónimo y no pseudónimo, por medio de un servicio de mezcla descentralizado llamado DarkSend⁹⁶. Ripple, en cambio, es un nuevo protocolo diseñado para realizar transacciones financieras globales de modo “seguro, instantáneo y casi gratuito” y es el primer *exchange* des-

centralizado⁹⁷. *Nxt* y *Peercoin*, entre otros atributos, son más sustentables para el medio ambiente ya que incorporan el *Proof-of-Stake*⁹⁸. Las variaciones son infinitas.

Por el momento, *Bitcoin* sigue siendo el líder indiscutido. En términos de capitalización de mercado, a comienzos de febrero de 2015 representaba más del 80% del universo de las criptomonedas, seguido por *Ripple* (12%) y *Litcoin* (2%)⁹⁹. Muchos observadores creen que logrará mantener la ventaja de *first mover* por haber sido el primer jugador del mercado. Este hecho le ha permitido generar una creciente red de usuarios y desarrollar un vibrante ecosistema a su alrededor. Más allá del costo que implica crear una nueva criptomoneda, cualquiera que quisiera superar a *Bitcoin* tendrá que vérselas con su poderoso efecto red, es decir, con el poder que le otorga la red de individuos, empresas, inversores e instituciones que operan con él, además de la red de minería que le brinda al sistema su enorme poder de procesamiento. Esto no significa que *Bitcoin* esté libre de riesgos. Es posible que surja una nueva generación de criptomonedas que corrijan las debilidades de *Bitcoin* o incorporen nuevas funciones. Otras amenazas incluyen fallas de seguridad, una reacción efectiva de las tradicionales instituciones financieras o incluso alguna ofensiva regulatoria coordinada de muchos países. De todas maneras, *Bitcoin*, como concepto y como protocolo, ha llegado para quedarse.

[94] Resolución 300/2014. Monedas Virtuales. Resolución N°70/2011. Modificación, Unidad de Información Financiera, 4 de julio de 2014. Acceso online: <http://www.boletinoficial.gov.ar/Inicio/Index.castle>.

[95] <https://litecoin.org/>.

[96] <https://www.darkcoin.io/intro.html>.

[97] <https://ripple.com/guide/#what-is-ripple>.

[98] <http://www.nxtcommunity.org/>; <http://www.peercoin.net/>.

[99] <http://coinmarketcap.com/currencies/views/all/> Datos del 1 de febrero de 2015.