Abril 2018 | Número 50 | ISSN: 2618-1703

Boletín de la Economía Mundial

Boletín de la Economía Mundial

El Boletín de la Economía Mundial es una publicación mensual que tiene como objetivo analizar y difundir lo que sucede en la economía internacional, a fin de brindar información y promover la reflexión y el debate para la toma de decisiones tanto en el área pública como en el sector privado.

Los temas tratados serán seleccionados en función del impacto sobre la economía argentina, para lo cual se tendrá en cuenta las cuestiones vinculadas con el comercio, las inversiones, el movimiento de capitales y el financiamiento, como así también la posición sobre los temas que nos importan de los organismos internacionales (OMC, FMI, BID, BM) y de las conferencias mundiales (Ronda Doha, G20, conferencias sobre medio ambiente y energía, desarrollo, etc.).

Cabe aclarar que el Boletín de la Economía Mundial se encuentra dirigida al público en general, por lo cual se posee una política de acceso libre y gratuito.

Editorial

El Boletín de la Economías Mundial es editado por la Escuela de Economía y Negocios de la Universidad Nacional de San Martín.

Los artículos publicados por el Boletín han sido seleccionados en función del impacto sobre la economía argentina, para lo cual se tendrá en cuenta las cuestiones vinculadas con el comercio, las inversiones, el movimiento de capitales y el financiamiento, como así también la posición sobre los temas que nos importan de los organismos internacionales (OMC, FMI, BID, BM) y de las conferencias mundiales (Ronda Doha, G20, conferencias sobre medio ambiente y energía, desarrollo, etc.).

Escuela de Economía y Negocios
Universidad Nacional de San Martín
Caseros 2241. San Martín. CP:1650. Provincia de Buenos Aires. Argentina
+54 11 4580 7250 int. 102 / 142.
E-mail: oem@unsam.edu.ar
Web: www.unsam.edu.ar/escuelas/economia/oem/boletines.asp
ISSN: 2618-1703

Criptomonedas: desarrollo, volatilidad y riesgos

Patricia Knoll y Anahí Viola
con la supervisión de Jorge Remes Lenicov

> **"Las monedas virtuales, tal vez más notablemente el bitcoin, han capturado la imaginación de algunos, han causado temor entre otros y han confundido al resto de nosotros". Thomas Carper, Senador de EE.UU.**

El mundo del dinero se está transformado. El vertiginoso avance de la informática y la digitalización de la economía están creando nuevos paradigmas de transacciones financieras y alternativas de capital. Un mundo sin dinero en efectivo y donde cualquier persona pueda transferir la propiedad de su dinero con un simple click, podría ser realidad en las próximas décadas.

En este nuevo mundo digital, las criptomonedas emergen como la gran estrella. En sólo una década se han convertido en un fenómeno global que mueve cientos de millones de dólares diarios. El bitcoin, la más conocida, incrementó su valor 260% solo en 2017.

Una criptomoneda es una representación digital de valor que puede ser intercambiada digitalmente. Su principal característica es que su emisión no es controlada por ninguna entidad o gobierno, y sólo se emite una cantidad previamente determinada y a una velocidad también definida con anterioridad y conocida públicamente. Funciona como medio de intercambio, unidad de cuenta y/o depósito de valor, pero no tiene estatus de moneda de curso legal. Cumple con las funciones anteriores sólo por acuerdo dentro de la comunidad de usuarios de la moneda virtual.

El precio de una criptomoneda se determina por el juego entre la oferta y la demanda. Su valor depende de la confianza que los participantes tengan sobre la calidad presente y futura de sus atributos para ser ampliamente aceptada como medio de pago, depósito de valor y unidad de cuenta frente a otras alternativas similares.

Esta exótica versión del dinero debe su nombre al método por el cual se genera: la validación de una transacción en este sistema se realiza mediante la resolución de un desafío criptográfico utilizando la tecnología Blockchain.

Blockchain es un libro de cuentas, una enorme base de datos, en la que se van apuntando todo tipo de transacciones. Todo funciona por consenso de las partes, y no se puede borrar ni modificar el pasado, ni tampoco operar fuera de las normas que se ha dado la propia red. Los nodos mantienen copias constantemente actualizadas de ese enorme libro de cuentas. Dentro de los nodos, se encuentran los *mineros*, estos realizan en sí las operaciones (que son vigiladas por los nodos en forma pasiva). Los mineros son procesadores que trabajan las 24 horas de los 365 días del año para resolver problemas informáticos a cambio de una retribución en criptomonedas. Estos problemas informáticos son complejos enigmas criptográficos que garantizan la seguridad de la red. Todas las operaciones que se realizan en la red se van agrupando en bloques, y para validarlas los mineros deben encontrar una especie de clave informática llamada hash. Cada vez que un minero encuentra un hash válido (debe reunir una serie de condiciones), se lleva, tras la comprobación de al menos el 51% de los mineros, 12,5 bitcoins (esta suma va cambiando). Así la cadena de bloques se actualiza constantemente, quedando los libros actualizados

ISSN: 2618-1703
Boletín de la Economía Mundial

en todos los nodos.

Normalmente cuando realizamos transacciones en internet, requerimos de un intermediario que valide cada transacción (con un costo asociado) para asegurar que efectivamente quien realice la transacción tenga el dinero. En cambio, blockchain permite que este proceso de validación sea distribuido entre todos los usuarios del sistema brindando el control a los propios usuarios, por medio del libro de transacciones. Como cada operación registrada en el blockchain se encripta (es decir, recibe un código formado por una combinación de números realizada por la computadora que sigue unas determinadas reglas para que el código sea válido), **en ningún momento interviene la mano del ser humano**, y por lo tanto la información contenida en cada bloque no sería pasible de manipulación o falsificación.

No solo el nombre de estas monedas está imbuido de cierto halo místico sino también la forma en que aparecieron. En 2008 una persona (o grupo de personas, no se sabe con certeza) que actuaba bajo el seudónimo de Satoshi Nakamoto publicó un paper a través de la Cryptography Mailing List titulado *"bitcoin: Un sistema de efectivo electrónico de Peer-to-Peer"*. En ese documento se detallaban los pasos para crear "un sistema para transacciones electrónicas que no dependa de la confianza". En 2009 Satoshi Nakamoto registra el primer bloque de transacciones (conocido como el bloque de genesis), creando así la red Bitcoin y la emisión de los primeros bitcoins. Luego de generar los primeros bitcoins (se estima que fueron millones), Nakamoto desaparece y hasta el día de hoy se desconoce su identidad. Antes de desaparecer, Nakamoto entregó, en cierto sentido, las riendas del proyecto al desarrollador Gavin Andresen, quien luego se convirtió en el desarrollador líder de bitcoin en la Fundación Bitcoin, que es lo más cercano a una cara pública oficial de Bitcoin.

Desde la aparición del bitcoin, han proliferado muchísimas otras monedas virtuales. Inicialmente eran sólo copias del código de Bitcoin con algunos cambios, y a estas monedas se las llamó "altcoins" (construcción simplificada de las palabras "alternative" y "coins"). Las Litecoins pertenece a esta categoría. Pero a medida que pasó el tiempo el mercado comenzó a introducir verdaderas innovaciones ofreciendo aspectos distintivos, como mayor privacidad o eficiencia o la posibilidad de hacer contratos inteligentes[1] (Ethereum).

Criptomonedas más conocidas[2]

Una nueva criptomoneda nace casi a diario, a menudo a través de una "oferta inicial de monedas" (ICO por sus siglas en ingles)[3]. CoinMarketCap, un sitio web, enumera alrededor de 1.400 monedas digitales o tokens (fichas), entre las que se incluyen UFO Coin, PutinCoin, Sexcoin e InsaneCoin. Para enero de 2018, alrededor de 40 de ellas tenían una capitalización bursátil de más de mil millones de dólares.

- Bitcoin: la más famosa y la que ha despertado la fiebre por las criptomonedas. Creada en 2008, está limitada desde sus orígenes a 21 millones de unidades, de las que ahora hay 17 millones en circulación. Usa tecnología blockchain, sus usuarios son anónimos, la controla una red de mineros que gestiona las transacciones y crea las monedas. Aunque es más lenta que otras monedas (solo hace diez transacciones por segundo) se usa primordialmente como moneda refugio para los inversores. Cuando ocurre algún disturbio en el mercado de bitcoins, el resto de las criptomonedas pierden valor en los mercados.

- Ether: conocida como Ethereum por ser el nombre de su plataforma, es la segunda en importancia. Fue creada en 2011. También funciona bajo tecnología blockchain pero se diferencia de Bitcoin en que no existe un límite de monedas. Funciona a través de smart contracts (contratos inteligentes), unos códigos de programación que democratizan digitalmente los acuerdos y por lo tanto aseguran su cumplimiento. Es 50 veces más rápido operar con Ethereum que con Bitcoin (las transacciones tardan menos de 20 segundos en realizarse).

- Ripple: vende software para mover dinero entre países; más de 100 bancos se han suscrito a su tecnología, basada en una moneda llamada XRP. Surgida en 2012, es la tercera en importancia. La gran diferencia de XRP es que no está basada en tecnología blockchain y por lo tanto no está descentralizada, no es libre, requiere conocer la identidad de quien opera con ella, es muchísimo más rápida que bitcoin (en seis segundos puedes enviar dinero a cualquier lugar) y por todas estas cosas se ve con mejores ojos por el mundo financiero. Dos entidades españolas como Santander y BBVA ya operan con ella. Existen cien mil millones de Ripples pero no todas están en circulación porque la empresa se guarda la mitad a modo de garantía.

[1]Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes. Cuando se dispara una condición pre-programada, no sujeta a ningún tipo de valoración humana, el contrato inteligente ejecuta la cláusula contractual correspondiente. Tienen como objetivo brindar una seguridad superior a la del contrato tradicional y reducir costos de transacción asociados a la contratación.
[2]Basado en información del sitio 20 minutos que puede consultarse aquí.
[3]ICO´s (Initial Coin Offering) hace referencia a una innovación que permite la financiación de proyectos o empresas en fases tempranas de desarrollo. Permiten a dichas empresas realizar una preventa de derechos sobre el proyecto. El concepto es similar al de OPV (Oferta pública de Venta) pero difiere en la regulación a la que está sujeta cada una y en el instrumento que se emite. En una ICO se emiten "tokens" (unidades) de criptomoneda y en una OPV, acciones o pagarés.

- Litecoin: creada en 2011 por Charlie Lee, exejecutivo de Coinbase, la plataforma en la que se adquieren la mayoría de las criptomonedas. Más barata, más ligera (las transacciones se hacen mucho más rápido), más fácil de encontrar (se creó para que en el futuro existan 84 millones de monedas). Se opera a través de blockchain. Su ventaja es precisamente la rapidez: procesa sus bloques cada 2,5 minutos en vez de cada 10 minutos.

- Bitcoin Cash: es una nueva versión del bitcoin (a estas bifurcaciones del protocolo original se las llama fork). El 1 de agosto de 2017 se llevó a cabo esta variación y todo aquel que tenía entonces bitcoins, pasó a tener esa misma cantidad en bitcoin Cash. Desde aquella fecha, ya operan de forma independiente. Algunos expertos la ven como el relevo de bitcoin, quizás no como valor refugio, pero sí como moneda transaccional ya que permite operaciones más rápidas y con menores comisiones.

- Dogecoin: Nació así en 2013, copiando la tecnología de Litecoin. Existen cien mil millones de monedas y es tan famosa que es la segunda más intercambiada después de bitcoin, la más barata en comisiones y es incluso más rápida que Litecoin.

- Iota: es la criptomoneda para el Internet de las cosas (IoT). Nació en 2015 y la gestiona una organización sin ánimo de lucro alemana que quiere convertirla en la moneda usada en el futuro para las transacciones de millones de aparatos conectados a la red. Por ejemplo, un frigorífico que lance órdenes de compra directamente al supermercado y efectúe los pagos en esta moneda. O una línea de producción que detecte la falta de stock y lance órdenes de compra pagadas con Iotas. En vez de usar tecnología de bloques, utiliza Grafo Acíclico Diricto (DAG).

- Dash: es una abreviatura de Digital Cash (moneda digital) se creó en 2014. Su diferencia respecto a otras monedas es que, aparte de la tecnología descentralizada y de la minería —que sí tienen monedas como bitcoin— permite realizar tanto transacciones instantáneas como privadas. Estas dos últimas funciones no las gestionan los mineros, sino que se tramitan a través de masternodes en un segundo nivel. También es ocho veces más rápida que bitcoin con 56 transacciones por segundo. Los expertos la consideran una de las monedas más seguras porque exige a sus masternodes tener al menos 1.000 dash para actuar como tales.

Cuadro N° 1. 20 principales criptomonedas. En dólares y %

Posición	Nombre	Capitalización de mercado* (en millones)	Precio*
1	Bitcoin	133.992	7.889,6
2	Ethereum	49.863	504,3
3	Ripple	25.857	0,7
4	Bitcoin Cash	12.949	758,2
5	Litecoin	7.531	134,2
6	EOS	6.854	8,6
7	Cardano	6.539	0,3
8	Stellar	5.611	0,3
9	IOTA	4.369	1,6
10	NEO	4.295	66,1
11	Monero	3.115	195,4
12	NEM	2.983	0,3
13	Dash	2.913	363,5
14	TRON	2.747	0,0
15	Tether	2.282	1,0
16	VeChain	1.739	3,3
17	Ethereum Classic	1.635	16,2
18	OmiseGO	1.472	14,4
19	Qtum	1.452	16,4
20	Binance Coin	1.352	11,9

* valores al 17 de abril de 2018.

Fuente: Cryptocurrency Market Capitalizations. https://coinmarketcap.com/

Otras monedas menos conocidas también han tomado vuelo. Monero y Zcash se centran en la privacidad. Stellar ha desarrollado un sistema para transferir fondos a bajo costo que es utilizado por organizaciones benéficas, especialmente en países pobres.

Según el creador de LiteCoin Charles Lee, antes de decidir en qué moneda invertir, uno debería estar atento a cuatro factores: innovación real, grupo de desarrolladores sólidos, promoción honesta y un correcto sistema de incentivos. Ya que si un equipo gasta más recursos en marketing que en tecnología, entonces queda claro cómo asigna sus prioridades y puede ser una inversión riesgosa.

¿Quiénes demandan bitcoins?

La Teoría subjetiva del valor plantea que el valor de un bien está relacionado con la actitud de la gente hacia el bien y no por las propiedades intrínsecas del bien. Una persona con sed no demanda agua si existen otras alternativas. Pero en el desierto, donde no existen tantas alternativas, el valor del agua aumenta. Entonces, el valor económico de un bien depende de las circunstancias.
Las criptomonedas satisfacen a aquellos que demandan un mercado financiero aparentemente desregulado y versátil con buenas perspectivas de ganancias.

¿Cuál es el mecanismo que rige las bases de datos de Bitcoin?

Una criptomoneda, por ejemplo el bitcoin, no se imprime como el dinero fiduciario, sino que se "extrae" mediante un proceso denominado "minería", utilizando la capacidad de computadoras conectadas a una red mundial distribuida de desarrolladores de *software* voluntarios[4].

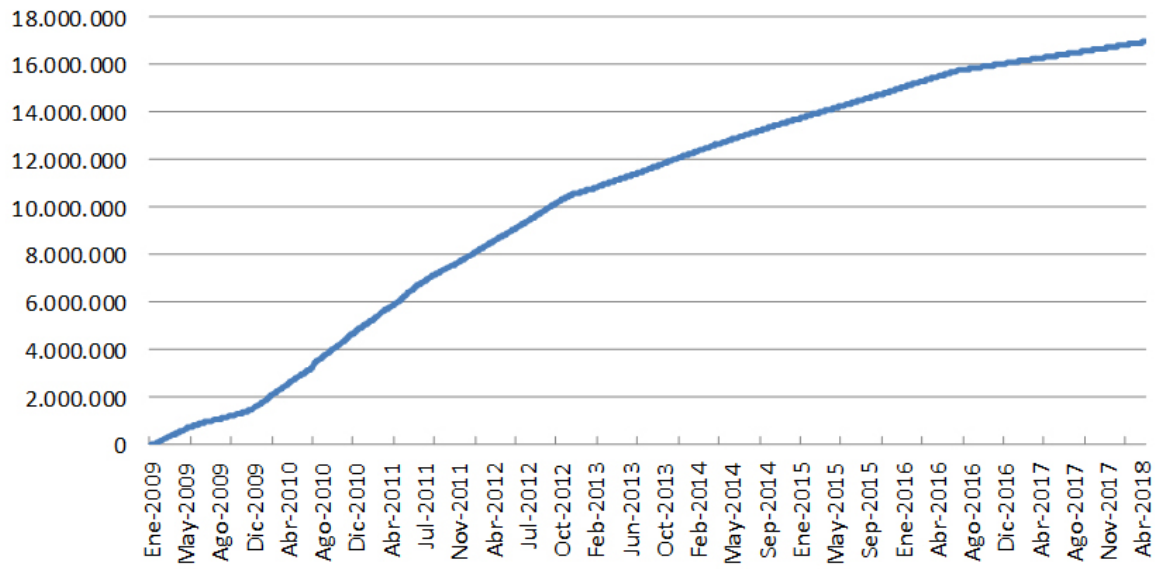
Esencialmente, Bitcoin es un archivo digital en el que se enumeran todas las transacciones que se han realizado en la red en una versión de lo que sería un libro mayor de contabilidad. Una transacción es un archivo que dice "A da X bitcoin a B" y está validada digitalmente[5] por una clave privada que posee A.
Esa transacción se trasmite de A hacia toda la red de pares por lo que el historial completo de todas las transacciones y, por lo tanto, del saldo de cada cuenta, se encuentra en cada uno de los ordenadores que conforman la red antes mencionada (P2P).

La transacción es conocida casi de inmediato por toda la red. Pero solo después de un tiempo se confirma. Mientras que una transacción no se haya confirmado, está pendiente y podría falsificarse (aunque esto es muy improbable). Pero cuando se confirma, esto sucede cuando la red recoge todas las operaciones realizadas durante un período establecido (habitualmente, cada 10 minutos) en una lista llamada "bloque", es inmutable, y no puede revertirse. Entonces pasa a formar parte de un registro inalterable de transacciones históricas, a esto es a lo que se llama tecnología blockchain (cadena de bloques).

Solo los mineros pueden confirmar las transacciones. Son ellos los que hacen funcionar la red de criptomonedas. Su trabajo es sellar las transacciones como legítimas y distribuirlas en la red. Después de que un minero confirma una transacción, se agrega en la base de datos de cada nodo convirtiéndola en parte de la cadena de bloques. La validación se realiza mediante la resolución de un problema criptográfico de mucha complejidad. Los mineros compiten entre sí para confirmar estos bloques. El primer minero que descubra la solución a ese problema, valida el bloque, lo "sella" y da comienzo a un bloque nuevo, que para ser validado requiere la resolución de otro desafío criptográfico. Cada vez que el sistema de un minero encuentra una solución que valida un bloque de operaciones, el minero recibe 25 bitcoins. Cada cuatro años aproximadamente, esta recompensa se reduce a la mitad.

[4] Esta tecnología se denomina *red peer-to-peer o red de pares* (P2P, por sus siglas en inglés) y consiste en una red de ordenadores que opera sin clientes ni servidores fijos a través de una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.
[5] La clave privada utilizada para demostrar identidad en cada transacción de criptomonedas sería el equivalente a la firma personal en el mundo físico pero prácticamente imposible de falsificar.

Gráfico N° 1. Bitcoins en circulación. En unidades*



Nota: el gráfico se refiere a los bitcoins que han sido minados, es decir, el stock de bitcoins disponibles en la red.
Fuente: Blockchain.com

La "minería de bitcoin" es una analogía a la minería del oro. Se le llama así porque los bitcoins están ocultos. En total hay 21 millones, pero a la fecha solo se han minado, es decir, descubierto, 17 millones. Como se dijo, a medida que una persona encuentra la solución de un desafío criptográfico complejo que valida un bloque de la cadena, es premiada con bitcoins. El día en que se hayan encontrado todos, no se generarán nuevos.

Comprar o minar, las dos formas de conseguir criptomonedas

Hay básicamente dos formas de conseguir criptomonedas. La primera, es recurrir a los mercados de valores internacionales, casas de cambio virtuales (que ya existen a nivel local) o brokers independientes. El proceso en líneas generales es simple: uno se contacta con la entidad vendedora, se establece una tasa de cambio (a nivel local generalmente es realizada al valor del dólar informal), se acuerda una forma de pago (transferencia bancaria, efectivo, intermediario digital, etc.), se envían las monedas a una billetera virtual (con una dirección criptográfica, como si fuese un CBU) y se realiza la transferencia virtual.

La segunda, ligada más a los programadores, es la minería comentada anteriormente. Este proceso implica armar computadoras especializadas, que resuelven algoritmos matemáticos y reciben como recompensa monedas virtuales. Este proceso puede ser realizado de forma independiente o mediante un grupo de mineros que trabaja de forma colectiva para conseguir más rápidamente las recompensas, lo cual es mucho más popular. Cada criptomoneda tiene un nivel de dificultad y una forma distinta de minado; en líneas generales la potencia computacional es determinada por dos factores: los procesadores y las placas gráficas de video.

No obstante, el hardware utilizado en la minería, con la evolución exponencial de la dificultad[6], fue progresando rápidamente y hoy ya no es rentable minar bitcoins con placas gráficas de video. El progreso de la nanotecnología permitió la creación de maquinarias especializadas (ASIC)[7] que son muchísimo más chicas y eficientes. Estas máquinas son fabricadas por unas pocas empresas en el mundo y tienen una altísima tasa de demanda, con listas de espera para poder adquirirlas. El funcionamiento de estos equipos implica un costo energético muy alto y, debido a que las rutinas de minería se complejizan cada vez más, este costo también tiende a elevarse con el correr de los meses.

[6]En la minería de bitcoins, existe un parámetro de dificultad que se recalcula cada 2016 bloques. Si la velocidad de la minería de bloques aumenta por el aumento de la capacidad de procesamiento, aumentará también de forma proporcional la dificultad para poder mantener el ratio de reparto de un nuevo bloque cada 10 minutos.
Eso significa que la capacidad de conseguir bitcoins con la minería no depende de la capacidad de procesamiento absoluta sino de la capacidad de procesamiento relativa que se tenga en relación a todos los otros mineros de bitcoins. Este sistema ha llevado a la evolución de la minería de bitcoin desde los CPU, hasta los ASIC.
[7]ASIC (Circuito Integrado para aplicaciones específicas) consiste en un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general. Se usan para una función específica.

La principal consideración al comprar un dispositivo ASIC es, como en cualquier inversión, el ROI (retorno de la inversión). Esto está determinado por la potencia de hash del dispositivo, es decir, la cantidad de bitcoins que puede generar diariamente, menos los costos de electricidad, los costos del grupo de mineros y la dificultad actual de la minería.

No obstante, si alguien desea comenzar a minar, puede hacerlo con otras criptomonedas, por ejemplo el Litecoin que todavía se puede minar con placas gráficas de video.

Actualmente también existen servicios profesionales de minería en la nube que utilizan tecnología de punta en lugares con precios muy bajos de energía. En vez de comprar el equipo y minar desde casa, se compra un contrato de minería en la nube y el proveedor es el que realiza el trabajo.

Costo energético de la minería

Aproximadamente 3.600 nuevos bitcoins son creados a diario a través del complejo proceso de la minería (que consiste en premiar con bitcoins a las computadoras que procesan complejas ecuaciones matemáticas a través de un software especializado). Se trata de miles de máquinas en todo el mundo trabajando día y noche sin parar, lo que implica un altísimo consumo de electricidad que no ha parado de crecer. La razón estriba en que a medida que los bitcoins se vuelven más valiosos, más y más máquinas se encienden para dedicarse exclusivamente a la tarea de fabricarlos.

El constante aumento de la dificultad para sellar transacciones y el crecimiento de los nodos que las verifican, hacen que sea difícil de estimar el verdadero costo de la minería. Sin embargo algunas estimaciones, como la realizada por el banco ING[8], señalan que el minado de un bitcoin conlleva un costo de 200 kWh, que es la energía que consume un hogar promedio en un mes. Por otra parte, el índice Digiconomist's bitcoin Energy Consumption estima el consumo anual para toda la red en 32,56 TWh (teravatios) en 2017[9]. Esto equivale al 0,13% del consumo total de electricidad mundial y significa que el minado de bitcoins consume más electricidad que 159 países.

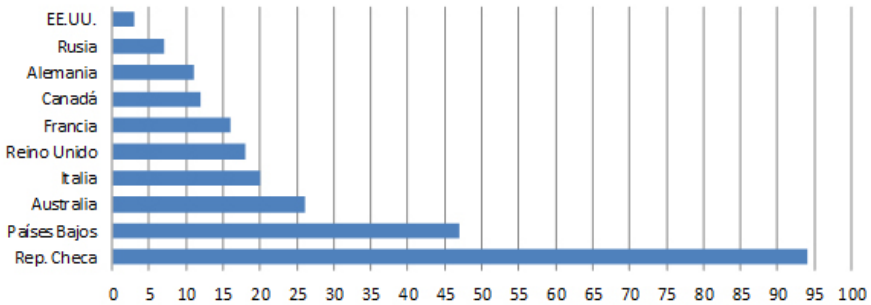
Si los mineros de bitcoin fueran un país, estarían en el puesto 61 en el mundo en términos de consumo de electricidad.

Sin embargo es muy difícil saber si estas estimaciones son correctas ya que no hay fuentes confiables reconocidas sobre el gasto de energía en monedas digitales como el bitcoin. Como, en teoría, cualquiera puede minar, resulta bastante difícil hacerse una idea general de todo lo relacionado con la criptomoneda, excepto su valor.

La fórmula que utiliza Digiconomist para calcular el consumo de energía se basa en las especificaciones de desempeño de la tecnología más empleada para la minería. Como punto de partida toma todos los ingresos de la minería, estima los costos operacionales de los mineros como un porcentaje de sus ingresos (60%) y los convierte en gasto por consumo de energía basado en los precios promedios de la electricidad.

Sin embargo, como el método recurre a varios supuestos y estimaciones, reconocidas abiertamente por el mismo Digiconomist, también tiene sus detractores. Algunos analistas aseguran que los supuestos están equivocados porque no se toma en cuenta el avance de las tecnologías para minar, que cada vez son más eficientes y que es erróneo afirmar que un 60% fijo de los ingresos por minería se gastan en electricidad.

Gráfico N° 2. Consumo energético para la minería mundial de bitcoins en comparación del consumo total de energía de distintos países. En %.



Nota: corresponde a la energía necesaria para la minería de bitcoins en todo el mundo, en comparación con el consumo energético de cada país.

[8]ING, Why bitcoin transactions are more expensive than you think, 2017
[9]Según un informe de "Power compare" disponible en https://powercompare.co.uk/bitcoin/

Hoy mucha gente utiliza el bitcoin como reserva de valor, es decir, como un lugar estable en el que colocar el dinero mientras que su uso como medio de pago todavía no se encuentra tan extendido. Por lo que algunos se preguntan si tiene sentido esta lógica de generar valor acumulando dinero en un sistema que conlleva un gran desperdicio ambiental y que no tiene ningún otro uso importante, al menos por ahora. Por supuesto, muchos no comparten esta inquietud.

Pero más allá de su potencial utilidad, o de como se quiera medir el consumo de electricidad del bitcoin y otras criptomonedas, hay algo en lo que todos concuerdan: como sucede con cualquier producto, físico o digital, su futuro dependerá de lo eficiente que sea su producción.

Criptodatos

- **Bitcoin es aceptada por más de 100.000 comerciantes en más de 92 países, de los cuales 6.000 tienen presencia física (Microsoft, Dell, PayPal, etc.)**
- **1.876 personas trabajan a tiempo completo en la industria de la criptomoneda, la mayoría en Asia-Pacífico y América del Norte.**
- **El 58% de los grandes grupos mineros están asentados en China. Estados Unidos ocupa el segundo lugar con 16%.**
- **Un 3% de la población de Estados Unidos es dueña de algún tipo de criptomoneda (es uno de los países con mayor penetración).**
- **1 de cada 5 universitarios en EE.UU. usa su préstamo estudiantil para invertir en criptomonedas.**

Riesgos del uso de las criptomonedas

Si bien el uso de este tipo de moneda tiene ventajas, también implica asumir algún riesgo personal y por otro lado, las criptomonedas pueden permitir el lavado de activos y la financiación de la actividad terrorista por las siguientes razones:

- Proporcionan un mayor nivel de anonimato respecto de los métodos tradicionales de pago sin efectivo.
- Se caracterizan por relaciones de clientes que no se conocen y esto permite la financiación anónima.
- Puede permitir transferencias anónimas, si el remitente y el destinatario no están adecuadamente identificados, cosa que ocurre generalmente.
- Los sistemas descentralizados son particularmente vulnerables a los riesgos del anonimato. Por ejemplo, las direcciones de bitcoin, que funcionan como cuentas, no tienen ningún nombre u otra identificación de cliente conectado, y el sistema no tiene ningún servidor central o proveedor de servicios.
- El protocolo de Bitcoin no requiere o proporciona la identificación y verificación de los participantes o genera registros históricos de las transacciones que están necesariamente asociadas con la identidad del mundo real. Esto es como medida de seguridad para los bitcoins, pero a su vez se puede utilizar para ocultar operaciones ilícitas.
- No hay ningún órgano de supervisión central para monitorear e identificar patrones de transacciones sospechosas. Muy pocos Estados ejercen control sobre estas transacciones.
- Se han registrado casos donde hackers informáticos realizaron secuestros virtuales de datos y han pedido el pago en bitcoins para liberarlos. La utilización de los bitcoins ayuda a realizar esto dado que la identidad de los poseedores de monedas virtuales es desconocida.

La falta de regulación internacional genera preocupación en diversos países ante la posibilidad de poder utilizarlas en operaciones ilegales. Es por esto que naciones como Bolivia, China, Ecuador e Irán prohibieron

su uso en los últimos años.

Por otro lado, la utilización de estas monedas implica asumir algún tipo de riesgo, como por ejemplo:

- Ser defraudados, puesto que no existe físicamente ningún organismo que respalde estos valores.

- Al usarlas como medio de pago, dado que su traspaso se realiza según la utilización de códigos encriptados, se corre el riesgo de realizar el pago y no recibir la mercadería. Esto puede suceder con cualquier medio de pago electrónico, pero a diferencia de los medios actualmente generalizados, el uso de criptomonedas no tiene ningún respaldo.

- Es muy alta su volatilidad, esto responde a diversos factores (ver "por qué es tan alta su variabilidad?"), y siempre implica un riesgo tanto para su uso en forma de inversión como para su uso como medio de cambio.
- Al pensarlo como una inversión, es muy complicado entender su funcionamiento, y eso siempre implica un riesgo para el inversor.

- Al ser el 100% moneda virtual, podría ser manipulada por los hackers (aunque no es una tarea para nada fácil). Esto es algo que los inventores de las criptomonedas ya tienen previsto con lo cual cada vez se generan más mecanismos para evitar esto. Aunque cada mecanismo que se genera implica una mayor demanda de tiempo y energía para cada transacción que se desea realizar.

Efecto impositivo

Las criptomonedas todavía se encuentran en un vacío legal puesto que en la mayoría de los países no se las considera como monedas, sino como algún tipo de activo generado entre privados, y es por esto que no les puede imponer los tratamientos impositivos que tienen las monedas de uso corriente. No se puede hablar de evasión puesto que no hay leyes para evadir…

Actualmente la mayoría de los países están adecuando sus normas para incluir a las criptomonedas dentro de los pagos de renta financiera. Al considerarlas como un activo del cual se obtiene una ganancia entre compra y venta (símil a las acciones), sus propietarios deben pagar impuestos en estos casos, aunque al ser muy difíciles de rastrear aún no se sabe si esta reglamentación será muy efectiva.

Este es un tema muy observado en la mayoría de los países puesto que las criptomonedas están creciendo a un ritmo vertiginoso, incluso se está planteando elaborar una legislación internacional para regularlas.
Un planteo que se escucha cada vez más fuerte es que actualmente su uso se extiende cada vez más como moneda de pago (aunque no sea reconocido oficialmente), con lo cual, tarde o temprano, los países y sus legislaciones se van a tener que adecuar a esta nueva realidad.

¿Por qué es tan alta su variabilidad?

Parte de su explicación radica en que las criptomonedas tienen una oferta fija (la cantidad estipulada de minado), y ante la creciente demanda del mismo, su precio sube abruptamente. Otra cuestión radica en que al no estar atadas a ningún bien físico o a ninguna entidad financiera que las respalde, el valor de las mismas solo se regula por medio de la oferta y la demanda, y con el boom de su exposición en los medios de comunicación, se hicieron de dominio público y creció vertiginosamente la demanda y no así la oferta por medio del "minado". Otra razón es el hecho de que aun no estan reguladas en la mayoría de los países; se estima que cuando los gobiernos centrales provean de una mayor claridad en su regulación, su precio será más estable.

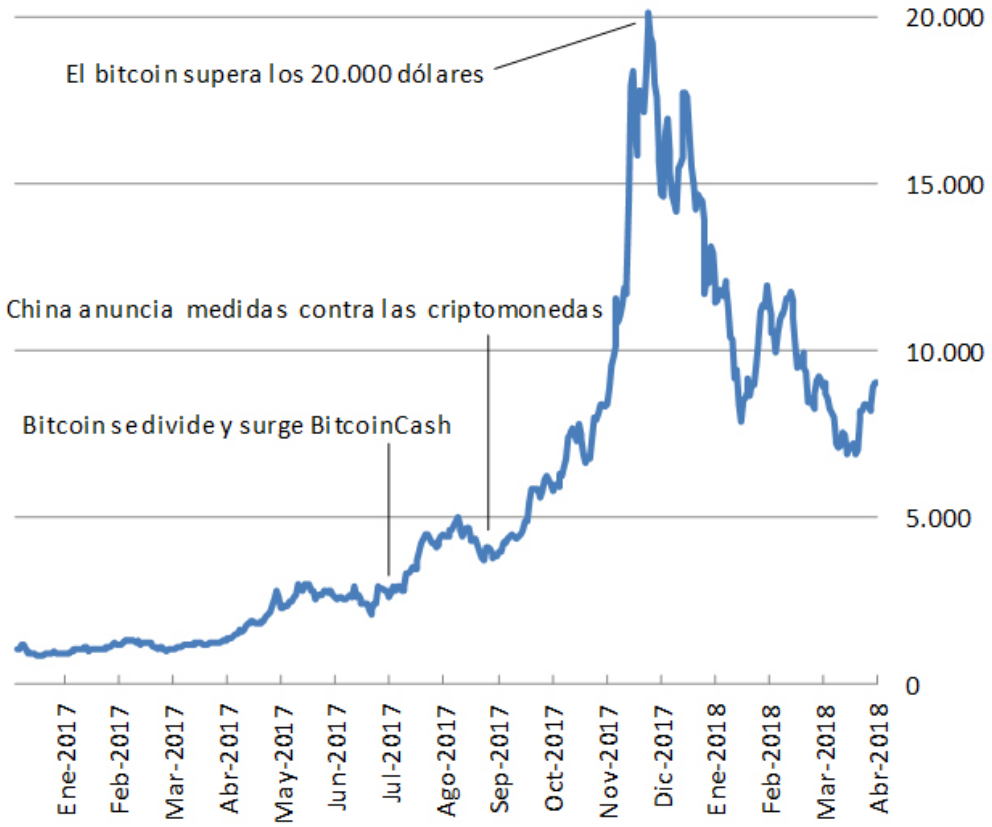
También se debe considerar el uso que se les da a estas criptomonedas puesto que se trata tanto de "monedas" de cambio como de activos para inversión, y estas dos cuestiones no son factibles en un mismo bien. Si se la piensa como inversión, no puede tener una rentabilidad del 0%, pero si se la piensa como moneda de cambio, es inaceptable que se incremente en un alto porcentaje puesto que pasa a ser una moneda pobre.

Al haber un crecimiento importante de la cantidad de criptomoedas que están en circulación, es de esperar que no todas tengan éxito, con lo cual se estima que para fines de 2018 muchas de ellas van a desaparecer.
Se debe tener cuidado con todo esto, ya que puede ser el inicio de otra de las famosas burbujas financieras que tantas veces se vieron en la economía mundial.

- Bitcoin (Ƀ): Hasta principios de 2017 representaba alrededor del 80% del mercado de monedas virtuales hasta que comenzaron a aparecer competidores que fueron ganando posición. Para fines de 2017 tenía el cerca del 60% del mercado y luego cayó a menos del 40% en enero de 2018. Su valorización en el mercado

el 6 de abril fue de 112 MM de dólares convirtiéndola en la más importante. Hasta mediados de 2017, las monedas virtuales tenían un comportamiento bastante constante, pero a partir de entonces pasaron a ser extremadamente volátiles con lo cual todavía no se puede definir una valorización en el mercado que considere de referencia. Los bitcoins pasaron de valer 1.400 dólares cada uno en mayo de 2017, a casi 20.000 dólares los primeros días de enero de 2018, para luego caer a 6.500 a principios de abril. Bitcoin ha logrado penetrar en cierta medida en el comercio electrónico *mainstream* pero el resto de las criptomonedas tiene una aplicación más limitada en el mundo real: son pocos los bienes y servicios que se pueden adquirir con ellas.

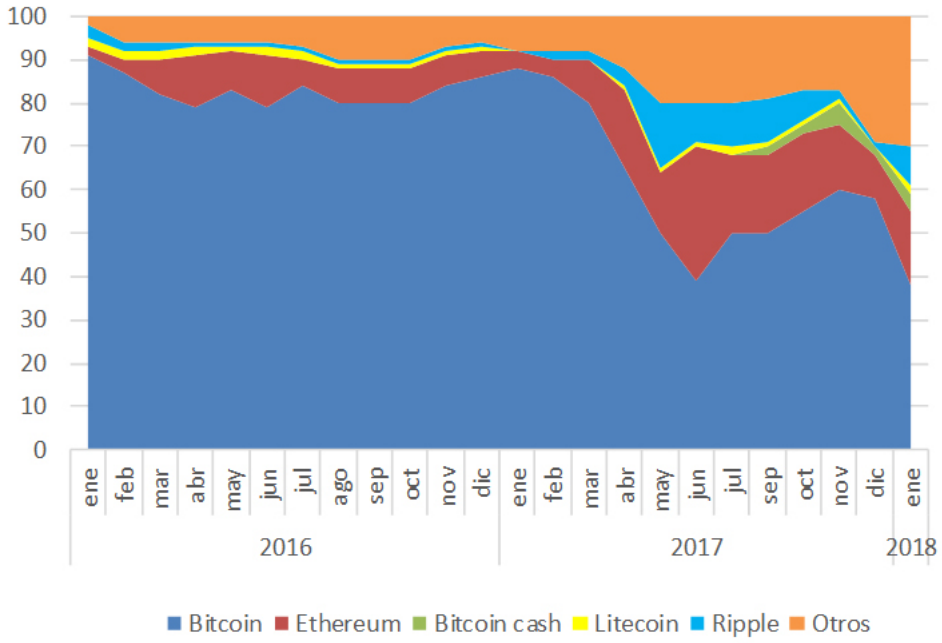
Gráfico N° 3. Bitcoins: evolución reciente de su valor. En dólares



Fuente: elaboración propia en base a datos de coinmarketcap.com

- Ether: alcanzó una capitalización de mercado de 137 MM de dólares en enero y cayó en abril a alrededor de 36 MM de dólares.
- Ripple: su capitalización de mercado saltó más de 40.000% en 2017, alcanzando casi 149.000 millones de dólares el 4 de enero, antes de caer nuevamente a 78.000 millones de dólares. En la actualidad sigue cayendo, siendo su capitalización de mercado para el 6 de abril de 18 MM de dólares.
- Bitcoin Cash: su capitalización pasó de USD 46 MM en enero de 2018 a 10 MM en abril de este mismo año.

Gráfico N°4. Principales criptomonedas, participación en el mercado. En %



Fuente: The Economist

China primera en minería

China representa más de dos tercios de la potencia de procesamiento global dedicada a la minería de criptomonedas. Además, alberga a algunos de los principales creadores de hardware para minar bitcoin.
El gobierno chino está tomando medidas para erradicar la industria de minado de bitcoin del país ante la preocupación que plantean el excesivo consumo de electricidad y el riesgo financiero. Algunos de los mayores mineros de China ya están trasladando sus operaciones al extranjero, EE.UU. y Canadá, están entre las opciones más populares.

Sin embrago, existen dudas sobre la eficiencia de las medidas restrictivas estatales, puesto que los gobiernos locales tienen fuertes incentivos para mantener a las grandes empresas mineras en sus regiones, dadas las enormes facturas de impuestos y de electricidad que pagan. Además las granjas mineras más pequeñas, especialmente en las zonas montañosas de las provincias de Sichuan y Yunnan, son casi imposible de ubicar.

Desarrollo y penetración en América Latina

La penetración de las criptomonedas en América Latina se registró recién a fines de 2016, muy por detrás de países como los EE.UU. o los europeos. Los países con mayor demanda fueron Brasil, Argentina, Venezuela, Colombia y México y en su gran mayoría se centraron en los bitcoins.

Venezuela presenta un caso excepcional en el mundo de las criptomonedas puesto que es el primer país con una criptomoneda propia, el Petro. Se anunció a fines de febrero de 2018 y en principio se está realizando la creación y preventa usando la plataforma de NEM. La decisión de lanzar esta moneda digital responde a la grave crisis económica –con importante devaluación incluida- que está atravesando el país en los últimos años. El mundo aun no la acepta como moneda (al igual que el resto de las criptomonedas), aunque el país latinoamericano la defiende puesto que fue lanzada en forma oficial. El riesgo del Petro justamente es que se devalúe a igual ritmo que la moneda de uso corriente en el país (bolívar).

Asimismo, Venezuela sigue siendo el territorio con mayor volumen transaccional de criptomonedas en América Latina, llegando incluso a alcanzar un volumen semanal de 100 millones de dólares en las 2 primeras semana de abril del corriente año. Por su parte, el volumen comerciado en Argentina alcanzó los 400 mil dólares mensuales y Brasil experimentó un mínimo aumento en el volumen intercambiado, alcanzando el millón de dólares mensual.

En Argentina, donde existe una fuerte tendencia a ahorrar en moneda extranjera, las criptomonedas, sin nacionalidad ni fronteras, comienzan a despertar un fuerte interés.

Algunos ejemplos de esto son la existencia de una Diplomatura en Criptoeconomías (ITBA) y el reciente desarrollo de Inbest Network. Esta plataforma, basada en tecnología blockchain, permite invertir en fondos

diversificados en las distintas criptomonedas. Para poder operar se debe comprar la criptomoneda propia del sitio, llamada IBST, y con ella invertir en los fondos de monedas virtuales que ofrece la plataforma.

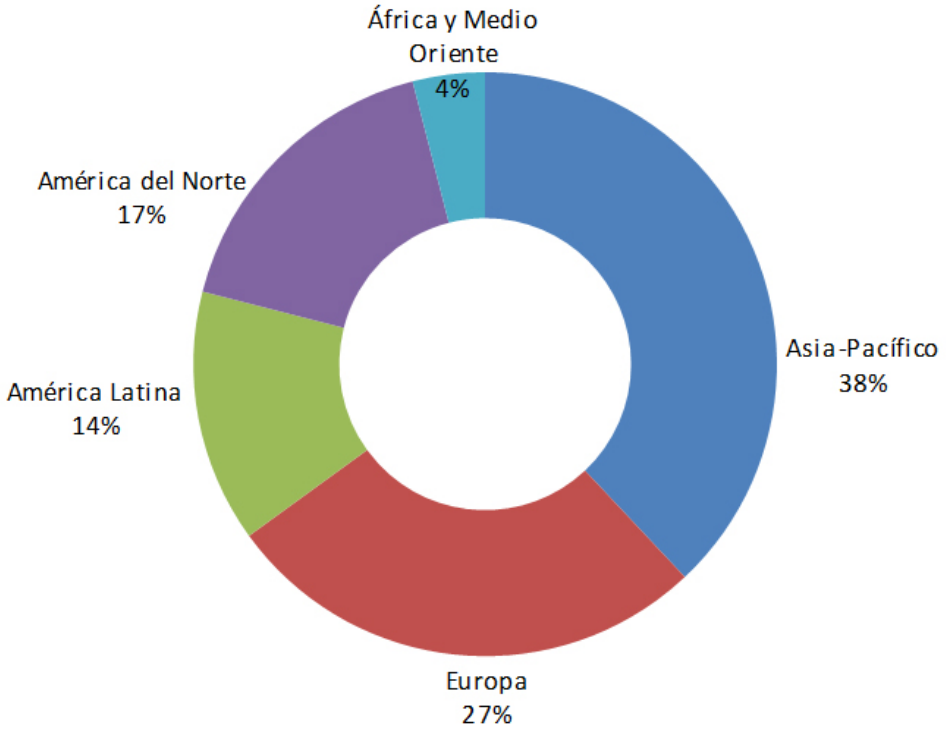
Asimismo, un grupo de argentinos lanzó Jasper, un proyecto de criptomoneda que usará un minado más sencillo y con menor consumo eléctrico. La compañía hará en el segundo semestre de 2018 una ICO por 330 millones de JasperCoins para financiar el proyecto. Se espera que la moneda tenga su red operativa en 2019.

Por otra parte, se espera que para finales de 2018 se encuentren operativos cajeros automáticos que operen con criptomonedas. Las primeras unidades llegarían a las ciudades de Buenos Aires, Córdoba y Jujuy. Los cajeros utilizarán la plataforma Octagon, que les permite operar con efectivo y criptomonedas. Por el momento, no se conoce el nombre de las empresas que implementarán el uso de estos cajeros, pero se habla de cadenas de supermercados y farmacias, locales de medios de pago y financieras no bancarias del interior.

¿Para qué tipo de transacciones se utilizan las criptomonedas?

Si bien la gran mayoría de las compras de criptomonedas se realizan como inversión, también es cierto que varias empresas han comenzado a aceptarlas como forma de pago (aunque su volatilidad ha determinado que algunas compañías se hayan echado atrás en su aceptación).

Gráfico N° 5. Criptomonedas: usuarios por región. En %

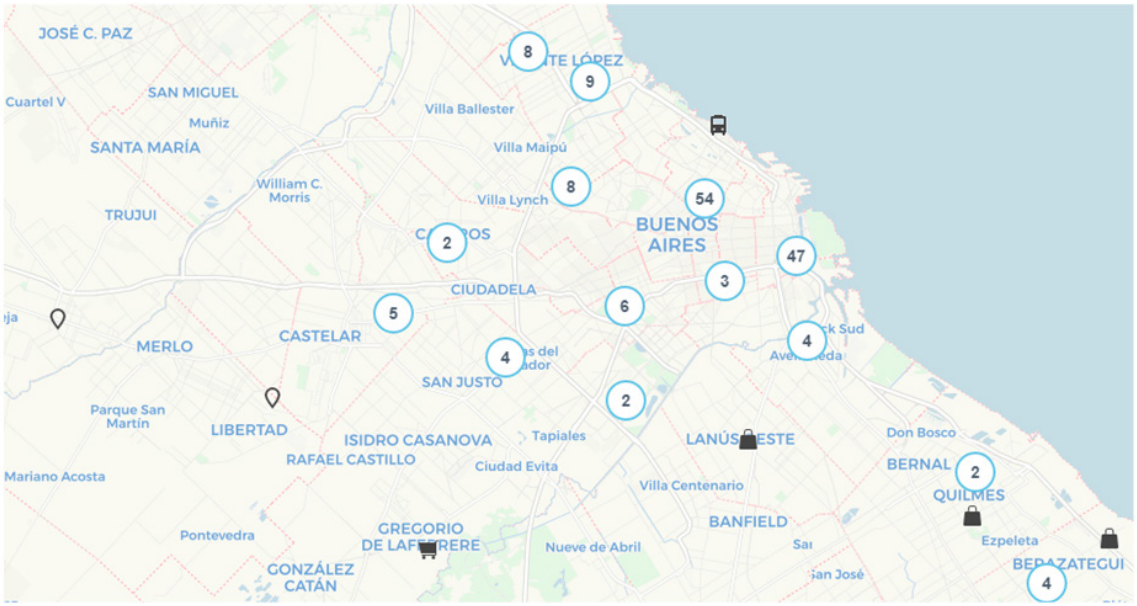


Fuente: University of Cambridge, Global cryptocurrency benchmarking study, 2017

Actualmente los poseedores de criptomonedas pueden gastarlas en la compra de películas aplicaciones y videojuegos, a través de Microsoft, o comprar paquetes turísticos o algunos productos en sitios online. También existen algunas aerolíneas que aceptan bitcoins como medio de pago: Air Lituanica y Air Baltic.

En Argentina, también se pueden pagar servicios turísticos en bitcoins (a través de sitios como Destinia) y la Ciudad de Buenos Aires posee más de 100 locales donde aceptan bitcoins, entre los que se encuentran: bares, una veterinaria, heladerías, locales de ropa, un almacén de vinos y quesos y hasta una academia de maquillaje y efectos especiales. No obstante, las ventas con bitcoins representan una cantidad marginal respecto a otros medios de pago.

Gráfico N° 6. Comercios que aceptan bitcoins en CABA y Gran buenos Aires, distribución



Fuente: Coinmap.org

Perspectivas

> **"¿Alguna de las criptomonedas de hoy será una Amazon o una Google, o terminarán como muchos de los motores de búsqueda ahora desaparecidos? El hecho de que estemos en una burbuja especulativa no significa que los precios actuales no puedan aumentar para un puñado de sobrevivientes." Steve Strongin (Goldman Sachs)**

Las criptomonedas formarán parte del futuro cercano aunque todavía no estén masivamente extendidas como medio de pago. Por otro lado, la metodología con la que se registran sus operaciones puede extenderse a otras áreas.

En 2017 proliferaron muchos proyectos relacionados con blockhain y criptomonedas. Muchos de ellos demostrarán ser inservibles. Sin embargo, como en el boom de las puntocom de los ´90, algunos proyectos se transformarán en valiosas firmas que permitirán crear productos y servicios que demostrarán ser útiles a largo plazo. Podría pensarse que surgirán más proyectos relacionados con transferencias de valor internacional (actualmente muy costosas), ofertas descentralizadas de microcréditos, servicios monetarios a quienes no estén bancarizados, como tarjetas de débito que permitan intercambios instantáneos de criptomonedas en cualquier local que las acepte, etc.

El 2018 podría ser otro año realmente interesante para la tecnología, hasta con mayor conciencia y adopción que en 2017.

Glosario

Altcoin: es una construcción simplificada de las palabras "alternative" y "coins". Podría traducirse, "monedas alternativas". El término altcoins se refiere a criptomonedas que derivan del código fuente de bitcoin. Estas derivaciones también son conocidas como forks. Todas las altcoins tienen en común que son implementaciones de monedas que se bifurcan desde bitcoin y difieren en los fundamentos de implementación de bitcoin.

ASIC: o circuito Integrado para aplicaciones específicas, es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general. Se usan para una función específica.

Blockchain: o cadena de bloques, es una base de datos compartida que funciona como un libro para el registro de operaciones de compra-venta o cualquier otra transacción. Es la base tecnológica del funcionamiento de Bitcoin, entre otras. Consiste en un conjunto de registros que están en una base de datos compartida on-line en la que se registran mediante códigos las operaciones. Al utilizar claves criptográficas y al estar distribuido por muchos ordenadores presenta ventajas en la seguridad frente a manipulaciones y fraudes. Una modificación en una de las copias no serviría de nada, sino que hay que hacer el cambio en todas las copias porque la base es abierta y pública.

Criptografía: en informática, es la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos), y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

Fork: o bifurcación del protocolo original, es la creación de un proyecto en una dirección distinta a la del proyecto principal u oficial a partir del código fuente de este ya existente. Esta práctica es de uso común en proyectos de código abierto o software libre. En las redes blockchain, las bifurcaciones son usadas tanto para crear nuevos proyectos partiendo de uno anterior, como para actualizar un proyecto en cuestión. Las nuevas criptomonedas que se crean por un fork o bifurcación de bitcoin, son las altcoins.

Hash: una función criptográfica hash- usualmente conocida como "hash"- o resumen criptográfico, es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. El más mínimo cambio que pudiera sufrir el bloque, alteraría dicha cadena, dando como resultado una completamente diferente. La idea básica de un valor Hash es que sirva como una representación compacta de la cadena de entrada. Lo importante de un resumen criptográfico es que sea fácil crear el valor Hash, pero sea prácticamente imposible deducir el contenido de la entrada leyendo el valor Hash. Para generar el Hash de las claves públicas y privadas de Bitcoin se utiliza el algoritmo de encriptación ECDSA (Elliptic Curve DSA).

ICO: acrónimo por "Initial Coin Offering", es decir, oferta inicial de monedas. Es un instrumento que se usa en el mundo de las criptomonedas para financiar el desarrollo de nuevos protocolos o proyectos. Por tanto una ICO es ofrecer a unos inversores iniciales las nuevas monedas a cambio de dinero.

Minería: proceso en el cual muchos ordenadores de una red P2P compiten por resolver problemas criptográficos complejos a cambio de una recompensa en criptomonedas.

Minero: los mineros son procesadores que obtienen los bitcoins como recompensa a la resolución de un problema matemático. Este reto matemático siempre es igual en su proceso pero las variables son diferentes y solo puede resolverse probando números al azar sin parar hasta dar con el resultado que se busca en ese momento. El primero que lo consiga se lleva la recompensa. Esto genera competencia y búsqueda de eficiencia mejorando los ordenadores para este objetivo.

Nodo: cada ordenador de una red P2P.

Red P2P: red peer-to-peer o red de pares (P2P, por sus siglas en inglés), es una red de ordenadores que opera sin clientes ni servidores fijos a través de una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Smart contract: programa informático que ejecuta acuerdos establecidos entre dos o más partes. Cuando se dispara una condición pre-programada, no sujeta a ningún tipo de valoración humana, el contrato inteligente ejecuta la cláusula contractual correspondiente. Tienen como objetivo brindar una seguridad superior a la del contrato tradicional y reducir costos de transacción asociados a la contratación. De forma esquemática, se implementan de la siguiente manera: se programan las condiciones, se firman por ambas partes implicadas y se "coloca" en blockchain para que el acuerdo no pueda modificarse.

Token: (en inglés, ficha, como por ejemplo las que se utilizan en las máquinas recreativas) unidad de valor emitida por una entidad privada. Un token tiene semejanzas con una criptomoneda, pero a la vez es un concepto más amplio. Es más que una moneda, ya que tiene más usos. Un token servirá para aquello que la persona u organización que lo diseñe y desarrolle decida.