BCV OZ ECONÓMICO 3
Banco Central de Venezuela
Departamento de Información
Boletín Económico
Mayo – Junio 2018 / Año 22

Criptomonedas: un acercamiento a su definición, estructura y mercado[1]

Autores: Johanned Dávila y Ricardo De Angelis-León

Palabras clave: criptomonedas, tecnología financiera, plataforma tecnológica.

En los últimos años, las criptomonedas han cobrado relevancia en el sistema financiero global, ya que representan un nuevo mecanismo que ha sido utilizado como medio de pago e inversión dado el desempeño de sus cotizaciones. De hecho, los gobiernos han mostrado interés en ellas, y las han convertido en tema de investigación y desarrollo por su posible impacto en la economía. En ese sentido, algunos países han introducido propuestas para la creación de criptomonedas propias y también marcos institucionales y legales para su control.

Este artículo trata sobre la tecnología necesaria para la creación de criptomonedas. Además, aborda la taxonomía del dinero desmaterializado expuesta por el Fondo Monetario Internacional (Dong & otros, 2016); así como la conceptualización de las criptomonedas, sus características y mercado.

A. Bases tecnológicas y estructura

I. Tecnología P2P (peer to peer)

Se trata de una red descentralizada de datos que permite el intercambio de información entre usuarios que se encuentran enlazados sin la necesidad de estar conectados a un servidor; es decir, las computadores se encuentran conectadas entre ellas y son, al mismo tiempo, clientes y servidores.

II. La cadena de bloques (blockchain) y sus implicaciones

El *blockchain*[2] ha sido aplicado en distintos ámbitos a las criptomonedas, tales como la banca, mercados financieros y de valores, mercados de materias primas, registro y verificación de datos y procesos de cadenas de suministros, entre otros.

De acuerdo con su aplicación en el proceso del *bitcoin*, la primera y más famosa criptomoneda, este sistema funciona proporcionando una especie de registro contable distribuido que almacena todas y cada una de las transacciones realizadas. Dentro de este ciclo se da una serie de pasos, a saber: a) la creación de un nuevo bloque (o registro) cada diez minutos, en el que el sistema guarda la información de las nuevas transacciones llevadas a cabo en ese período; b) en un proceso aleatorio, se asigna usuarios de la red para que verifiquen las nuevas transacciones y aseguren que las características de estas sean únicas; c) de existir consenso en el paso anterior, el bloque se almacena en el sistema, tras lo cual genera una cadena que lo conecta linealmente con todas y cada una de las transacciones pasadas; d) los usuarios que definen y dan las características al nuevo bloque proceden a distribuirlo por la red para que cada miembro guarde una copia exacta de la cadena de registros, actualizándola cada vez que se genere un nuevo bloque, en un proceso cíclico.

El *blockchain*, además, usa un sistema criptográfico, lo que implica que cada transacción esté resguardada por claves públicas y privadas que cifran la información, lo que permite que únicamente aquellos usuarios dueños de dichas claves privadas puedan acceder a los detalles y, al mismo tiempo, la red pueda usar las claves públicas para la verificación.

A manera de ejemplo, se puede considerar la operación entre dos usuarios. El usuario A firma la transacción con su clave pública y privada, aparte de agregar la llave pública del usuario B[3], con lo que este último debe proporcionar sus datos para poder cerrar la operación con éxito y recibir el monto. Es decir, ambos usuarios realizan transacciones solo proporcionando sus claves públicas y privadas, mientras que otros usuarios del sistema verifican el proceso.

B. Definición

I. Taxonomía del dinero desmaterializado

En una concepción simple, las monedas virtuales son representaciones de valor, las cuales son emitidas por desarrolladores privados, estando denominadas en sus propias unidades de cuenta. Estas disponen de una serie de características: se puede acceder a ellas y ser obtenidas, almacenadas y transadas de manera electrónica. Esta concepción cubre un amplio rango de unidades virtuales: desde los puntos virtuales con los que se adquieren bienes y servicios (cupones *online* o millas de aerolínea) y monedas con respaldo en materias primas como el oro, hasta las conocidas criptomonedas como el *bitcoin*.

De acuerdo con un estudio sobre las monedas virtuales (Dong y otros, 2016), el dinero desmaterializado comprende entre sus características dos elementos clave: por un lado, la representación digital de valor (ser monedas), lo que permite la transferencia entre partes; por el otro, los mecanismos de pago y liquidación subyacentes[4].

Ante estos dos elementos fundamentales, se pueden encontrar otras subcaracterísticas, como el esquema de convertibilidad, es decir, si el entorno en que operan permite o no volver a las monedas FIAT[5] (de curso legal), siendo de esquema abierto (con libre convertibilidad), o de esquema cerrado (con convertibilidad restringida)[6].

Las monedas virtuales pueden operar bajo modelos centralizados, descentralizados o híbridos, lo que determina la forma en la que se construye el sistema interno de estas. En los descentralizados no existe un emisor o controlador único (como un banco central) y se opera con una estructura donde los participantes verifican las transacciones y pagos; al tener una función (trabajo) específica, aquellos son recompensados por el sistema con monedas recién creadas; esta es la figura del minero. Por su parte, en los sistemas híbridos algunas funciones son realizadas por una autoridad central y otras se distribuyen entre los participantes.

II. Criptomonedas

Son monedas virtuales creadas a partir de métodos de encriptación para la garantía de las operaciones.

Se trata de la primera red descentralizada de pagos punto a punto impulsada por sus usuarios sin autoridad central o intermediarios[7], lo que permite que dos partes interesadas realicen transacciones directamente entre ellas sin la necesidad de un tercero de confianza. Las transacciones, computacionalmente irreversibles desde el punto de vista informático, protegen a los vendedores contra el fraude, y los mecanismos de custodia de rutina pueden implementarse fácilmente para proteger a los compradores[8].

III. Bifurcaciones de las criptomonedas (forks)

Dentro del entorno global de las criptomonedas se han generado cambios en los protocolos internos que las rigen, dando paso a estructuras y dinámicas que han derivado en nuevas monedas. A estos cambios o bifurcaciones se les conoce como *forks* y no son más que el proceso de consenso de los usuarios de la red para introducir nuevas dinámicas (que generan mejoras o no) al sistema subyacente. Las bifurcaciones pueden ser de dos tipos: I) en las que toda la red acepta el cambio y mantiene la criptomoneda y sus protocolos; II) en la que se dan cambios fundamentales que modifican protocolos esenciales, pudiendo dar paso a nuevas criptomonedas.

Han habido bifurcaciones fuertes ante las que no todos los usuarios de la red estuvieron de acuerdo y optaron por los protocolos originarios, tal ha sido el caso de *Bitcoin Cash* y *Ethereum Classic*. Por otro lado, las monedas alternativas o *altcoin* se consideran bifurcaciones fuertes de código fuente, en las que se cambian las reglas fundamentales y protocolos de otras monedas y se abre paso a nuevas monedas, por ejemplo *Litecoin* y *Peercoin*, entre otras que funcionan con entornos y cotizaciones propias. En este sentido, la creación de una criptomoneda implica, por lo general, la oferta inicial de moneda (ICO, por sus siglas en inglés), que no es más que una oferta pública de *tokens*[9].

IV. Monedero o billetera digital (wallet)

Se trata de un sistema digital que permite almacenar información relacionada con pagos, montos y contraseñas. Dado que es posible instalar el *wallet (software)* en celulares, computadoras personales, *laptop* o tabletas, entre otros dispositivos, no se requiere intermediarios financieros para realizar transacciones electrónicas desde cualquier parte del mundo.

La billetera digital funciona como una cuenta bancaria, cada una es identificada con una dirección electrónica mediante la cual se pueden recibir y hacer pagos o transferencias.

C. Principales características de las criptomonedas

Entre las principales características de las criptomonedas se pueden destacar las siguientes: I) la mayoría son descentralizadas, es decir, no son controladas por ninguna entidad financiera; II) no son embargables, por lo tanto, no existe la posibilidad de congelar o cerrar cuentas arbitrariamente; III) hay bajo costo transaccional, no es necesario tener intermediarios debido a que la criptomoneda se transfiere directamente entre personas; IV) no es necesario revelar cuentas bancarias o números de tarjetas de débito o crédito; V) son encriptadas, lo que hace, hasta ahora, imposible la duplicación o falsificación; y VI) pueden ser canjeadas por monedas FIAT.

I. Tabla comparativa (materias primas, criptomonedas y dinero)

	Bitcoin	USD	*Commodity (oro)*
Factores económicos de la demanda			
Valor intrínseco	No	No	Sí
Posibilidad de reclamo a los emisores	No	Sí	No
Tenedor legal	No	Sí	No
Uso como medio de cambio	Pequeño, pero se ha incrementado en el comercio minorista online	Sí	Sí
Uso como unidad de cuenta	No	Sí	Sí
Uso como reserva de valor	Sí, sujeto a riesgo en el tipo de cambio y expectativas de confianza	Sí, sujeto a riesgos de inflación	Sí, sujeto a ciclos de precios
Estructura de la oferta			
Monopolio/Descentralizado	Descentralizado	Monopolio	Descentralizado
Fuente de oferta	Privado	Público	Privado/Público
Cantidad	Inflexible	Flexible	Inflexible
Reglas de oferta	Programa de computadora	Reglas con base a la inflación	Costos de oportunidad de minería
Cambio en las reglas (emisores)	Sí, con la aprobación de la mayoría de los mineros	Sí	No
Costos de producción	Alto (costo eléctrico)	Bajo	Muy alto (minería)

Fuente: Dong y otros (2016).

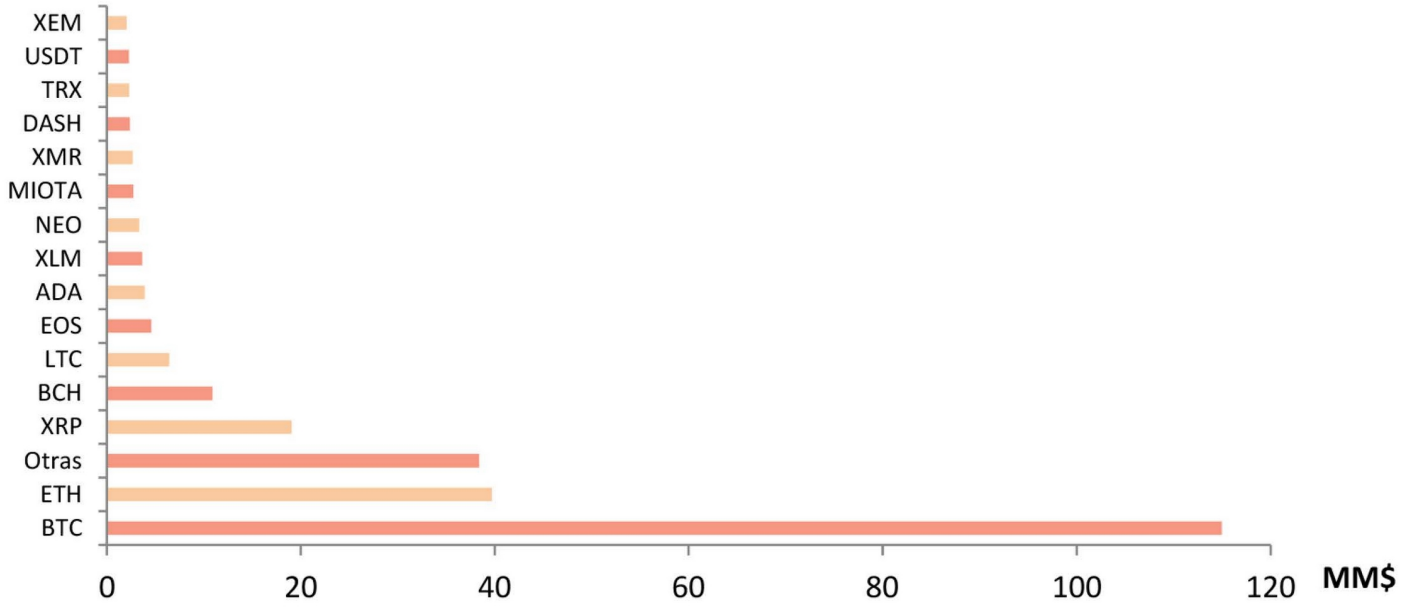
D. El mercado de las criptomonedas

Existen más de 1.500 tipos de criptomonedas[10], que se transan entre usuarios en mercados no regulados a través de billeteras electrónicas, mientras que solo el *bitcoin* se transa en ámbitos regulados tradicionales como el Mercado de Opciones de Chicago (CBOE)[11].

De acuerdo con datos de Coin Market Cap, el mercado de las criptomonedas, al primer trimestre de 2018, ascendía a USD 259.390 millones, liderado principalmente por el *bitcoin*, el cual mantuvo al cierre del período una capitalización de USD 115.000 millones, que representa 44% del total. Lo anterior constituye un tercio de la mayor capitalización que registró la principal criptomoneda del mundo en su punto más alto en diciembre de 2017, cuando rozó los USD 330.000 millones[12], lo que analistas determinaron como el punto de inflexión de una carrera especulativa de compra-venta que derivó en una caída sostenida en la cotización de la totalidad de las monedas que componen el mercado.

Según diversas firmas de análisis financiero como FXTM, Think Markets y el Banco de Inversión Goldman Sachs, el desplome del mercado de las criptomonedas se debió sobre todo a la entrada en vigencia de regulaciones en los mercados asiáticos, principalmente en China y Corea del Sur, donde se implementaron medidas para regular el llamado crecimiento irracional.

Capitalización de mercado de las principales criptomonedas



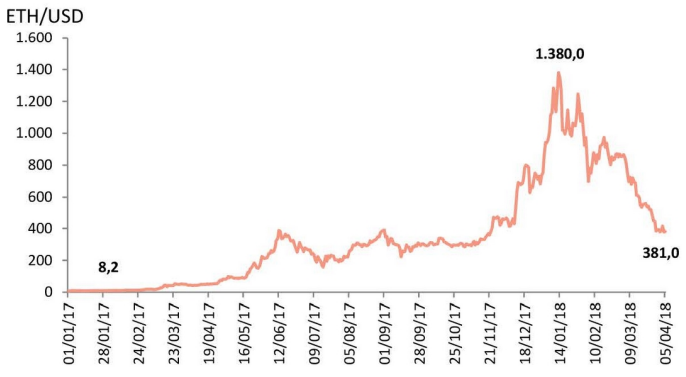
Fuente: Coin Market Capital.

La cotización del *bitcoin* al 05/04/2018 se ubicó en 6.765 BTC/USD, y aunque mostró una tasa de variación anual de 493,1%, las variaciones mensual y diaria mostraron un importante descenso de 40,75% y 0,35%, respectivamente, desde diciembre de 2017, cuando se ubicó en 19.187 BTC/USD.

Similar tendencia se observa en el caso de *Ethereum*[13] (plataforma descentralizada que permite crear contratos inteligentes a partir de una cadena de bloques), cuya cotización mostró una variación anualizada de 740,1% y variaciones mensuales decrecientes de 55,1%.

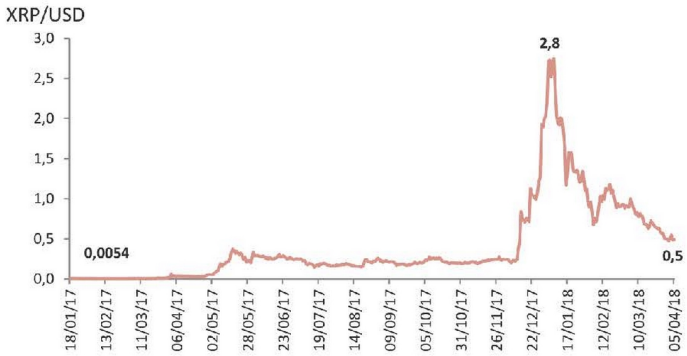
***Bitcoin*/USD**

***Ethereum*/USD**



Asimismo se destacan, debido a su importancia en el mercado, las cotizaciones del *Ripple*[14] (basado en la tecnología *blockchain* que conecta a los bancos, proveedores de pagos e intercambios de activos digitales), con una tasa de variación anualizada de 1.280%, superior a las de *Bitcoin* y *Ethereum*.

***Ripple*/USD**



Notas

[1] Este artículo forma parte de una serie dedicada al tema de las criptomonedas. En el próximo número del *BCVoz Económico*, como parte de una estrategia para afianzar la comprensión sobre esta área innovadora, se tratarán las criptomonedas y los sistemas de pago.

[2] Durante el año 2017, la tecnología *blockchain* fue uno de los temas más buscados y nombrados en todos los espacios informativos. Para ponerlo en perspectiva, Reuters realizó un reporte sobre el tema a principios de 2018, donde aseguraba que en las plataformas de las grandes distribuidoras de noticias, como PR Newswire, arrojaba cerca de 2.000 resultados con notas de prensa solo para el primer trimestre de 2017, cifra que asciende a 97.000 resultados si se usa la sección de noticias del buscador Google para el mismo período.

[3] En este punto puede imaginarse la emisión de un cheque en el que no aparecen los datos personales del emisor, sino una clave compuesta de caracteres alfanuméricos que solo él posee, pero los demás pueden ver y, en lugar de su firma, otra clave única que solamente él conoce. Además de haber escrito en el apartado "Páguese a la orden de" la clave pública del usuario final.

[4] En particular, el rol de las criptomonedas dentro del sistema de pagos será abordado en una investigación subsecuente a esta publicación.

[5] Luego del abandono del patrón oro, el dinero pasó a usar el sistema FIAT o fiduciario, que en latín tiene una traducción literal en torno a la palabra fe, por lo que divisas como el dólar, euro o la libra están respaldadas por la solidez y confianza en sus sistemas económico, financiero y fiscal.

[6] Un ejemplo de esquema cerrado son los entornos virtuales o videojuegos, en los que se transan monedas pero con una convertibilidad en un solo sentido, no permitiendo el retorno a las FIAT. En el entorno abierto existen tipos de cambio que varían con los flujos de oferta y demanda, y posibilitan el ir y venir de monedas virtuales a FIAT sin restricción.

[7] Mayor información en Web Bitcoin.org.

[8] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", documento que en 2008 teorizó por completo los mecanismos del bitcoin.

[9] Los *tokens* son monedas virtuales emitidas en su totalidad (no minables), para recaudar capital con la intención de financiar el proyecto de una criptomoneda.

[10] Mayor información en https://coinmarketcap.com (06/04/2018)

[11] Es el mercado de futuros y de opciones más grande del mundo. También es un líder en el desarrollo de nuevos productos financieros e innovación tecnológica, especialmente en comercio electrónico.

[12] Comportamiento seguido por la mayoría de las criptomonedas, que lleva la capitalización total del mercado por encima de los USD 600.000 millones.

[13] Mayor información en https://www.ethereum.org

[14] Mayor información en https://ripple.com

Referencias

Arango, C. y Bernal, J. "Criptomonedas". Documentos Técnicos y de Trabajo. Banco de la República de Colombia. Colombia, 2017.

BitCoin.org. "¿Cómo funciona?" Fecha de consulta 05/04/2018. https://bitcoin.org/es/como-funciona

Bloomberg. "Goldman Sachs pronostica que la mayor parte de las criptomonedas caerá a cero". Fecha de consulta 07/04/2018. http://www.portafolio.co/internacional/la-mayor-parte-de-las-criptomonedas-caera-a-cero-goldman-514065

Coin Market Cap. "Top Cryptocurrencies by Market Capitalization". Fecha de consulta 06/04/2018. https://coinmarketcap.com/es/

Dong, H. y otros. "Virtual Currencies and Beyond: Initial Considerations". International Monetary Fund, Staff Discussions Note. Enero 2016. SDN/16/03.

ESE Business School. "Bitcoin y Criptomonedas". Centro de Estudios Financieros, Universidad de los Andes. Colombia, agosto 2017.

Kelly, J. y Dreyfuss, G. "Bitcoin, other cryptocurrencies tumble on government crackdown worries". Fecha de consulta: 06/04/2018. https://www.reuters.com/article/uk-markets-bitcoin/bitcoin-other-cryptocurrencies-tumble-on-government-crackdown-worriesidUSKBN1F50UV

Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System". Fecha de consulta 05/04/2018. https://bitcoin.org/bitcoin.pdf

Reuters. "Are you ready for blockchain?" Fecha de consulta: 04/04/2018. https://www.thomsonreuters.com/en/reports/blockchain.html

Presidente
Ramón Lobo Moreno

Primera Vicepresidenta Gerente (E)
Sohail Hernández Parra

Segundo Vicepresidente Gerente (E)
José Salamat Khan Fernández

Gerente de Comunicaciones Institucionales
Yosendy Chirguita Peña

Grupo Editor
Omar Mendoza, Yosendy Chirguita Peña, Francisco Vallenilla, José Contreras, Amarelis Vásquez

Jefe del Departamento de Información
Francisco Moreno Pérez

Diseño y Diagramación
Hady Abousaed Chuffi - Karelys Coconubo

Corrección
Departamento de Publicaciones

ISSN: 1315-1407