¿Qué son las criptomonedas? (primera parte)

25 de octubre de 2019

Autor: Arnie Zareei Bogoya
Miembro del equipo de trabajo del Proyecto Edufinet

“Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value”.

Eric Schmidt, Executive Chairman of Google.

El dinero surgió antes del inicio de la historia escrita, y, como consecuencia de ello, cualquier testimonio sobre su origen está basado en conjeturas[1].

Existen numerosas evidencias del uso del trueque como medio de intercambio; en general, podían ser objeto de trueque las mercancías utilizables por sí mismas, pero también otras con menos facilidad para su uso pero atractivas formalmente, como conchas y abalorios. En algún momento que no podemos determinar con precisión, el sistema de trueque se transformó en otro monetario.

Históricamente, el precedente a la acuñación de monedas metálicas fue la ficha de arcilla (y otros materiales similares) en los antiguos imperios de Egipto, China, India y Babilonia[2]. Estas fichas (*tokens*) representaban un producto, pudiéndose canjear en el almacén[3] o intercambiarse en los mercados como si fuesen, idealmente, el propio producto representado. Incluso podían entregarse a los trabajadores como forma de pago.

Las monedas más antiguas, en sentido estricto, de las que se tiene conocimiento, se acuñaron, combinando oro y plata, en el siglo VII antes de Cristo, en la península de Anatolia (actualmente Turquía), específicamente, en el Reino de Lidia[4].

El sistema de papel-dinero, en cambio, fue introducido por la Dinastía Song en China durante el siglo XI, y se conoció en Europa en el siglo XIII gracias a comerciantes y viajeros como Marco Polo o Rubruquis[5].

El extraordinario desarrollo de la tecnología en la segunda parte del siglo XX permitió que el dinero se pudiese representar masivamente por medio de anotaciones en cuenta, con un peso cada vez mayor de la representación digital sobre el dinero total en circulación.

Con la llegada de Internet, las tiendas en línea entraron en escena permitiendo a los consumidores comprar o vender en los mercados sin acudir físicamente a los mismos. La primera operación conocida se realizó el 11 de agosto del año 1994, con la venta de un CD de Sting por 12,48 dólares, con el uso de *software* encriptado para enviar el número de tarjeta y el CVV2[6].

En 2009 Satoshi Nakamoto, un seudónimo tras el que se oculta una persona o un grupo de personas, desarrolló la primera criptomoneda descentralizada llamada *Bitcoin*, que utiliza una función criptográfica denominada SHA-256[7] dentro del esquema *proof-of-work*[8].

Veamos un ejemplo de funcionamiento de un sistema de pagos descentralizado de esta naturaleza:

1. Nos encontramos en un sistema descentralizado llamado *Edufi System* que utiliza *Edufis*, una moneda virtual, donde no existe un Banco Central (como la Reserva Federal o el Banco Central Europeo) que actúa en coordinación con el sistema bancario para registrar la compensación y la liquidación de los pagos. Y estos *Edufis* se almacenan en la cartera virtual o local de cada usuario.
2. @Alicia le envía a @Carolina 1 *Edufi.* Al no existir un Banco Central que actúa coordinadamente con las entidades de crédito, ¿cómo se verifica la operación entre @Alicia y @Carolina?
3. Para confirmar y verificar la realidad y la validez de los respectivos apuntes de adeudo y abono, existe una base de datos que reúne todas las transacciones dentro de *Edufi System*, que funciona como un libro mayor. Para que no se pierda toda esta información, aquí es cuando entra en juego la tecnología del *Blockchain*[9]: esta información se recoge en una cadena de bloques compartida por todos los usuarios. Cuando se realiza una transacción, la información se añade a la cadena como un nuevo bloque, que se suma al conjunto de datos.
4. ¿Cómo puede @Alicia y @Carolina añadir esta nueva transacción al nuevo bloque? Aquí es cuando nace la figura del minero, que es el encargado de crear el bloque.
5. Esta información, como se puede suponer, es muy sensible, y, por ello, para completar una nueva transacción, los mineros deben de competir entre sí para descifrar el problema criptográfico que será

la llave para crear un nuevo bloque.

6. Si el minero descifra el problema, todos los demás usuarios que están dentro del sistema, comprobarán si es correcta la solución (*proof-of-work*); como consecuencia, si más de la mitad han verificado que es correcta, se añadirá la transacción a la cadena de bloques.
7. Se ha completado la transacción y el minero recibe una compensación por su trabajo. Pero, ¿quién le paga al minero? Es recompensado con *Edufis* que se han generado al crear un nuevo bloque con todas las transacciones y una comisión voluntaria por parte de @Alicia para que incluya la transacción que ha iniciado.

En consecuencia, una criptomoneda (*cryptocurrency*) es una moneda digital divisible (por ejemplo: 1 Satoshi = 0,00000001 *Bitcoin*) que se almacena en una cartera en línea (*online*), funciona con la tecnología de bloques *blockchain* y, como su nombre indica, es un medio de pago, siempre que sea aceptado por las dos partes implicadas, con el que el usuario puede realizar transacciones con el uso de una criptografía muy fuerte: SHA-256.

En junio de 2019, como se muestra en el Imagen 1, el mercado de criptomonedas se componía de 2.610 criptomonedas, y alcanzaba una capitalización de 290.000 millones de dólares (como las seis empresas más grandes del IBEX-35, aproximadamente), siendo el volumen de operaciones efectuado en un día de, aproximadamente 50.000 millones de dólares. Estas cifras son significativas si tomamos en consideración que el volumen promedio diario de negociación del IBEX-35 se sitúa en torno a 150 millones de euros, y que su capitalización es de aproximadamente, 570.000 millones de euros.

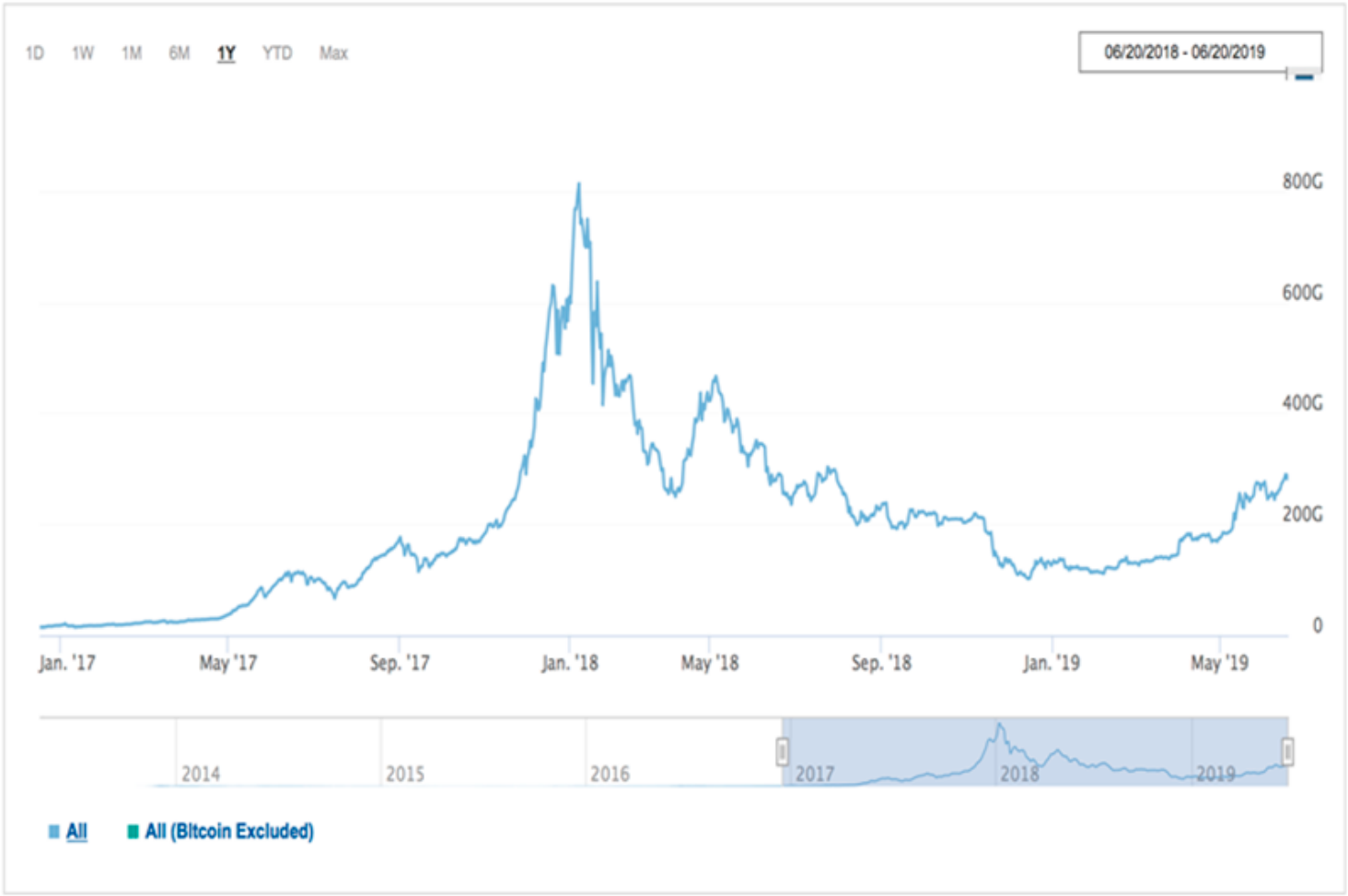

Imagen 1. Volumen de operaciones del mercado de criptomonedas entre enero de 2017 y principios de junio

de 2019. Fuente: https://www.investing.com/crypto/charts.

Como se puede observar en la Imagen 1 y en la tabla 1, el mercado de criptomonedas tiene una alta volatilidad. El 31 de diciembre de 2016 el mercado total de criptomonedas tenía una capitalización de 17.000 millones de dólares, un año más tarde, el 31 de diciembre de 2017, alcanzó la cifra de 610.000 millones, con un aumento del 3.347,58%. El 7 de enero de 2018, solamente siete días después, la capitalización aumentó un 33,40%, llegando así hasta 813.000 millones de dólares. A final de año disminuyó un 84.55% hasta los 125 mil millones y seis meses después aumentó un 130,82% hasta los 290.000 millones de dólares.

Día	Capitalización de mercado total	Variación momento anterior	Variación desde 31/12/2016
31/12/2016	$ 17.696.800.000,00		
31/12/2017	$ 610.112.000.000,00	3347,58%	3347,58%
07/01/2018	$ 813.871.000.000,0	33,40%	4498,97%
31/12/2018	$ 125.705.397.047,00	-84,55%	610,33%
10/06/2019	$ 290.152.320.287,00	130,82%	1539,58%

Tabla 1. Variación de la capitalización total del mercado de criptomonedas entre 31 de diciembre de 2016 y 10 de junio de 2019. Fuente: elaboración propia, con datos tomados de investing.com/crypto.

Observando tanto la gráfica del mercado como la del *Bitcoin*, Imagen 2, se me viene a la cabeza la Imagen 3 de Jean-Paul Rodrigue, en la que puede apreciar las fases de una burbuja financiera. Es difícil augurar lo que sucederá, son una realidad y por eso es importante conocer sus ventajas y desventajas que explicaremos en una segunda parte.

Imagen 2. Cotización del Bitcoin entre mayo de 2017 y julio de 2019. Fuente: https://www.investing.com/crypto/bitcoin/btc-usd.

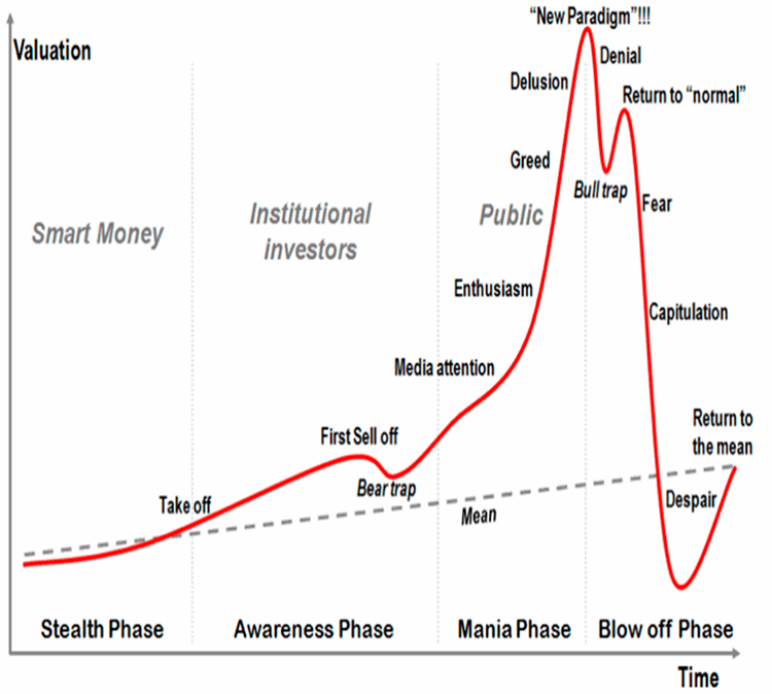

Imagen 3. Fases de una burbuja. Fuente: http://marketpredict.com/articles/mp-bubblecycle.htm.

Autoría de la imagen: freepik

---

[1] Keynes, J.M. (1930). Tratado sobre el dinero. Volumen I, página 13.

[2] Denise Schmandt-Besserat, Tokens: their Significance for the Origin of Counting and Writing. Accesible en el siguiente enlace: https://sites.utexas.edu/dsb/tokens/tokens/

[3] Estos imperios disponían de almacenes donde se podían almacenar las mercancías.

[4] https://www.britishmuseum.org/explore/themes/money/the_origins_of_coinage.aspx

[5] Moshenskyi, Sergii (2008). History of the weksel: Bill of exchange and promissory note, página 55.

[6] Para más información puede consultar la siguiente palabra en el glosario de Edufinet: http://www.edufinet.com/glosario/word/583

[7] La función hash es un algoritmo creado por la Agencia Nacional de los Estados Unidos que transforma una información conjunta, como puede ser un documento de texto, en un solo valor de longitud fija (el "hash").

[8] El esquema o sistema *proof-of-work* o prueba de trabajo en español es la primera puerta de verificación en el sistema *Blockchain.*

[9] Para más información puede consultar el siguiente artículo: https://blog.edufinet.com/que-es-el-blockchain-y-que-funciones-tiene/