¿Qué pasa con «bitcoin»?

Desde las primeras monedas acuñadas hace más de 2000 años, la revolución tecnológica ha hecho surgir las criptomonedas (con bitcoin a la cabeza) como una necesidad al creciente comercio vía internet. Su valor de uso y la confianza serán claves para el desarrollo de las mismas, más allá de los problemas que ya se están encontrando en el camino.

Nereida González @nereidaglopez | *Consultora del área de Análisis económico y de mercados de Afi*
Fernando Rojas @Ferojas | *Consultor de Banca en el área de Servicios Financieros de Afi*

Las primeras monedas oficiales de las que se tiene constancia en la historia se remontan sobre el siglo VII o VI antes de Cristo en una región de la actual Turquía. Nacen como respuesta de darle un sentido a los trueques que se realizaban en esa zona eminentemente habitada por comerciantes. Para desarrollar su función, se necesitaba una manera de contrastar, de generar confianza para evitar los posibles fraudes. Para ello, los reyes acuñaban las monedas con sus caras literalmente moldeadas en ellas para evidenciar de dónde procedían dichas monedas y dónde eran válidas. Era una forma de generar esa confianza a los comerciantes.

Las monedas proliferaron rápidamente a lo largo de los siglos, mostrándose como una forma de generar comercio. Conforme iban creciendo las diferentes civilizaciones, se iban generando más necesidades sociales a que los diferentes estados debían dar respuesta. Sin embargo, la confianza se truncó por diversas razones que hicieron necesaria la creación de instituciones que garantizaran que la moneda que se estaba utilizando constaba con el respaldo necesario para poder confiar en ella. Por ello (entre otras razones), en el siglo XVII nace en Suecia el que se puede considerar como el primer Banco Central.

Por lo tanto, la creación de los bancos centrales nace como respuesta a la generación de una confianza perdida en las monedas en circulación. Con el respaldo de un banco central, se podría comerciar con esa moneda en partes del mundo donde se confiase en el país que la sustentaba.

Desde este momento, aunque posteriormente diversos estados declararon la bancarrota y arrastraron a estos bancos centrales tras ellos, es el sistema más o menos coordinado que hemos tenido hasta el siglo XXI.

iStock1/Thinkstock.

En estas mismas páginas se han tratado diversos temas que están cambiando la forma de percibir el mundo y, más concretamente, las finanzas (*Blockchain, Sandboxes, Fintech,...*). Los cambios comentados se están produciendo de manera rápida, tanto que ya se habla de una cuarta revolución industrial.

Internet ha sido una revolución. Desde los años 70 del siglo pasado en el que se crea, hasta los 90 donde se generaliza, hasta el primer decenio del siglo XXI donde forma parte permanente de nuestras vidas, se han desarrollado tecnologías que hacen posible el tratamiento de información en tiempo real, contactar con diferentes partes del mundo en cuestión de segundos y compras de cualquier producto que incluso pueden enviártelo en el día.

Recordemos que la moneda nace por una necesidad eminentemente comercial, ligado a una relación de confianza en la misma entre las partes que comercian. El *bitcoin* nace en 2009 como una necesidad co-

mercial vía internet, pero también como respuesta a una creciente desconfianza en los Bancos Centrales que daban esa confianza a las monedas en circulación desde el siglo XVII.

¿Qué es el bitcoin?

Ya hemos comentado por qué nace el *bitcoin*, así como otras miles de monedas virtuales o «criptodivisas» como pueden ser Ethereum, Litecoin... que pueden competir con el *bitcoin* o colaborar con la misma.

La tecnología que subyace a las monedas comentadas es el denominado Blockchain, como comentábamos en un artículo anterior en el número 174 de esta revista, que principalmente es un libro de contabilidad que sirve para contrastar las transacciones realizadas entre partes, cada una verificada y sellada por una tercera parte independiente que no es una autoridad estilo Banco Central, sino los propios participantes. La cadena de bloques está disponible para la consulta de cualquiera, pudiendo reconstruir la secuencia histórica de las transacciones realizadas.

Los participantes son los que «emiten» los *bitcoin*, ya que este no se emite como puede hacerse de manera tradicional, sino que se «mina». El proceso de minado lo puede realizar cualquier usuario con un ordenador, al que se le denominaría «minero», con programas informáticos dedicados, basados en la verificación de la cadena de códigos que representan el historial de transacciones de *bitcoin*. Una transacción no es considerada válida hasta que no existe un consenso entre los mineros, lo que garantiza anonimato, integridad y que este *bitcoin* no pueda ser duplicado.

Esta tecnología es la que origina la confianza entre los participantes del uso de las monedas virtuales. Como se ha comentado con anterioridad, la confianza es la principal cualidad que debe tener una moneda para que se haga uso de ella, ya que, sin ella, ningún participante aceptaría dicha moneda de cambio.

En el párrafo anterior nombramos **dos características que están definiendo las innovaciones y el futuro: el valor de uso y la confianza**. La primera de ellas es el paradigma que contrarresta el valor intrínseco de las cosas. El ejemplo más claro es el de los móviles: les damos un valor por lo que podemos hacer con ellos, su valor de uso, no por el valor de los materiales (cristal, aluminio, etc...) que forman ese objeto.

Al igual que pasó con las monedas fabricadas de oro y plata, que dejaron paso a los billetes por los múltiples envilecimientos de las mismas, ahora el valor físico de los billetes podrá dar paso al valor de uso que tendrán las criptodivisas.

Analizando la segunda, es decir la confianza, recordemos que las monedas tuvieron en la confianza la cualidad principal que definía su valor de uso, y por ende, su utilidad a la hora de comerciar.

La confianza se ha descrito tradicionalmente como una forma subjetiva de percibir una característica, habilidad, fuerza, honestidad en relación a una cosa o persona. En relación a cualquier tipo de tecnología innovadora que impacte en las preferencias de los consumidores, podemos considerar que estas deben contar con tres tipos de confianzas: **confianza tecnológica, confianza social y confianza institucional**.

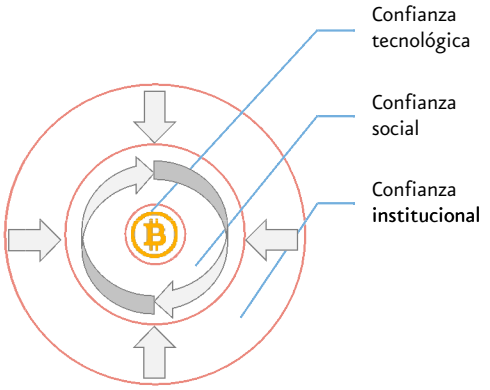
En relación a la **tecnológica**, es importante destacar que los individuos deben creer que el uso de la tecnología es necesario para su día a día. Los atributos que debe tener esa innovación se resumen en las ventajas del uso de la misma, las expectativas de uso y la percepción por parte del usuario de sus habilidades.

En relación a la **confianza social**, esta deriva del hecho de que el uso pueda conllevar un incremento del bienestar de todos los usuarios. Dentro de la confianza social se podría identificar cuatro atributos que la definirían: la disposición a la confianza, la confianza percibida, algunos factores en determinadas situaciones que se presentan en la sociedad y los atributos compartidos por los individuos.

Por último, una innovación debe tener una **confianza institucional** para generalizar su uso, vinculada a la intensificación del poder de relación que pueda realizar.

Suponiendo que se generalice su uso, consideramos que el *bitcoin* cumple, o puede cumplir con estas condiciones en el futuro, excepto el factor de la confianza institucional, ya que una de las cualidades que cumple el *bitcoin* es que es un sistema descentralizado; y no sólo eso, sino que además involucra a las partes interesadas en el uso, es decir, los mineros, los usuarios, los comerciantes y cambistas por monedas tradicionales.

NIVELES DE CONFIANZA EN LA TECNOLOGÍA *BITCOIN*



Fuente: *Afi; Sas, Corina; Khairuddin, Irni Eliana: «Exploring Trust in Bitcoin Technology: a Framework for HCI Research».*

¿Qué dificultades está teniendo?

No obstante, el *bitcoin*, como toda novedad tecnológica, está afrontando diferentes dificultades que se han ido presentando en su desarrollo. Algunas de ellas son las siguientes:

• **Velocidad de transacciones**. Una de las principales críticas que ha estado recibiendo el *bitcoin* desde sus usuarios es la velocidad en que las transacciones se pueden validar (o ejecutar). A modo de ejemplo, Visa procesa en torno a 150 millones de transacciones al día, una media de 1.700 transacciones por segundo. *Bitcoin*, en cambio, procesa solamente siete transacciones por segundo.

Además, a medida que los usuarios del *bitcoin* se han ido incrementando, la velocidad ha caído hasta el límite de que una transacción podría llevar días hasta que se completase ante la cantidad de bloques de información que se necesitan incorporar a la cadena. Este podría ser uno de los grandes problemas en el desarrollo y uso a nivel universal.

Poniendo el problema en cifras, los bloques de información que procesa *bitcoin* se generan cada 10 minutos y tienen un peso limitado a un megabyte de máximo. Las soluciones a este problema podrían pasar por reducir la cantidad de información que necesita ser verificada en cada bloque o incrementar el volumen de los bloques de datos.

Para corregir este problema, *bitcoin* decidió, a mediados de julio de este año, incorporar una nueva tecnología, conocida como SegWit2x que lo soluciona parcialmente a través de la reducción de información necesaria para validar un bloque de información. Este sistema «elimina» la firma digital[1], haciendo una verificación indirecta de la misma, sin necesidad de hacer una descarga de datos, lo que suponía cerca del 65% del consumo de energía del sistema de verificación. El resultado de esta implementación lleva a duplicar el peso que un bloque de datos puede soportar, agilizando las transacciones.

No obstante, la eliminación de esta firma digital podría incrementar el riesgo de generación de bloques de datos falsos, reduciendo la seguridad del proceso de generación de *bitcoins*.

• **«Desdoble» del *bitcoin***. Ante este eventual problema de seguridad en la generación de *bitcoins* originales, algunos mineros decidieron comenzar un camino diferente aunque paralelo: *Bitcoin Cash*. Ambas criptodivisas comparten el mismo histórico (cadena y transacciones) hasta el 1 de agosto de 2017. En consecuencia, aquellos usuarios que antes de esta fecha disponían de *bitcoins*, ahora tienen un *Bitcoin Cash* por cada *bitcoin* en posesión.

• **¿Burbuja?** El rápido ascenso del precio del *bitcoin* (que ha pasado de 1.000 dólares a más de 4.000 sólo en 2017 con una rentabilidad del 314%) ha levantado ciertas sospechas sobre la posibilidad de que se esté generando una burbuja.

Hace unas semanas, Jamie Dimon, director ejecutivo de JPMorgan, manifestaba su opinión de que el *bitcoin* es un fraude, comparándolo con la burbuja de los tulipanes que sufrió Holanda en el siglo XVII[2]. El gusto por las flores exóticas llevó a una gran euforia por los tulipanes de los Países Bajos, que sufrían variaciones en su apariencia, existiendo versiones multicolores, que las hacían aún más exóticas. Este es uno de los motivos que se achacan a una posible burbuja del *bitcoin*: una demanda creciente por un activo relativamente novedoso cuyo funcionamiento puede ser, en cierto modo, desconocido.

Evolución del precio del *bitcoin* desde su creación

(dólares por *Bitcoin*)

Fuente: *Afi, Bloomberg.*

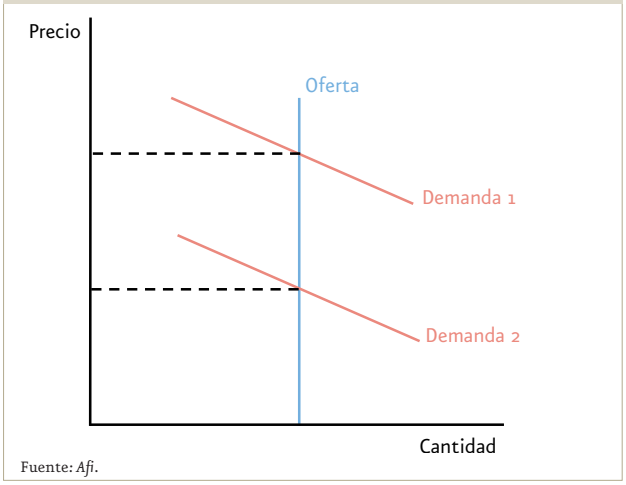
En el caso del *bitcoin*, Jamie Dimon mostraba su escepticismo sobre la voluntad de los países de permitir el uso de esta criptodivisa sin una supervisión estatal. Esto precisamente lo pudimos ver en el caso de China, país que prohibió el *trading* con *bitcoins* hace apenas un mes. Los motivos de esta decisión podrían ser dos: controlar la masa monetaria que se mueve en el país (motivo que mencionaba Dimon en su entrevista) o una nueva medida de control de capitales.

Como se ha mencionado alguna vez en estas páginas, China ha tenido, de forma estructural, determinados controles al libre movimiento de capitales. Muchos de los usuarios de *bitcoin* en China utilizaban este activo para poder sacar dinero del país, lo que podría justificar el afán de las autoridades chinas para restringir el uso de esta criptodivisa que, como hemos comentado, escapa a cualquier control gubernamental.

Más allá de los problemas... perspectivas de futuro

Frente aquellos que opinan que el verdadero valor del *bitcoin*, lejos de considerar los 4.000 dólares en los que cotiza en mercado, realmente es cero, se sitúan aquellos que piensan que podría llegar a valor 10.000 dólares (y por qué no más). Como todo precio, estará determinado por la demanda, pues la oferta, aunque aún es creciente, estará limitada en una cantidad máxima de 21 millones de *bitcoin*. Un uso generalizado de esta criptodivisa podría llevar a que la burbuja nunca explote, aunque su precio podría seguir siendo volátil: la evidencia muestra

ESQUEMA DE MERCADO CON OFERTA PERFECTAMENTE INELÁSTICA



Fuente: *Afi*.

que el precio del petróleo, mercado más inelástico, suele ser más volátil que otros mercados con mayor elasticidad.

No obstante, esto estará condicionado al uso que pueda tener y la confianza que los agentes otorguen a esta criptodivisa. En este aspecto, las autoridades y gobiernos jugarán un papel clave, pues serán los responsables de determinar el marco regulatorio adecuado.

A la espera de ver cómo se desarrollan estos dos factores, podríamos volver a tener novedades en el entorno del *bitcoin* tan pronto como noviembre. En ese mes se implementará por completo la nueva plataforma de SegWit2x y se alcanzará el tamaño máximo que los bloques podrán tener (2 megabytes). En este momento, se baraja la posibilidad de que se pueda generar un nuevo desdoble del *bitcoin* y se genere una nueva criptodivisa, lo que puede provocar alguna convulsión en su valor de cotización.

En resumen, aunque aún puede existir cierta incertidumbre y desconocimiento sobre el mundo de las criptodivisas, si algo es seguro es que su desarrollo no se frenará, aunque vendrá de la mano del impulso que se haga desde los usuarios, los empresarios y las instituciones ::

[1] Una firma digital es un mecanismo criptográfico que permite al receptor del mensaje pueda determinar la identidad originadora de dicho mensaje y confirmar que no ha sido alterado desde que fue firmado por su originador.

[2] https://www.cnbc.com/2017/09/22/bitcoin-jpmorgans-jamie-dimon-lays-into-bitcoin-again.html