Cod. 8708 | Economía del cambio tecnológico | 5306.99 Otras

Las criptomonedas (Bitcoin) y Blockchain

Cryptocurrencies (Bitcoin) and Blockchain

Pablo García-Bringas[1] y Giuseppe Psaila[2]
[1] Universidad de Deusto (España)
[2] Universidad de Bergamo (Italia)

DOI: http://dx.doi.org/10.6036/8708

Tras la publicación en el ejemplar de nuestra Revista DYNA correspondiente a septiembre/octubre de 2017 de **BLOCKCHAIN: Retos y oportunidades más allá del bitcoin**, *se han suscitado, por algunos de nuestros lectores, varias preguntas que hemos trasladado a los autores y que éstos, amablemente, nos han respondido de forma asequible, incluso para los no especializados. Dada la actualidad y los diversos puntos de vista generados alrededor del tema, nos abstenemos de cualquier juicio de valor respecto a los citados productos.*

Agradecemos a sus redactores, Pablo García Bringas y Giuseppe Psaila, la pronta respuesta a nuestra solicitud.

¿Podría cualquiera crear una criptomoneda?

El valor de una moneda reside en la confianza que los usuarios depositan en el avalista de la misma, en su creador, normalmente un Banco Central a instancias de un gobierno.

Bitcoin (así como otras criptodivisas aparecidas después) busca y consigue el objetivo fundamental de no depender de una entidad central, de ningún Banco Central y de ningún Gobierno. Crea confianza mediante la percepción de robustez que transmite a los usuarios el algoritmo matemático en torno al cual se construye la moneda, y siempre al margen de entidades centrales.

Dadas estas dos premisas, sí, es posible que un agente con unos ciertos recursos, no necesariamente muy elevados, despliegue toda la infraestructura necesaria para activar una criptomoneda. La puesta en marcha de una plataforma informática para este fin es algo muy abordable, en efecto. Otra cuestión es la confianza real que esto generaría en el mercado, ya que el interés de muchos usuarios reside precisamente en la no existencia de agente central (con eventuales intereses individuales).

¿Necesita autorizaciones administrativas y/o tener algún tipo de respaldo financiero?

No, criptomonedas como Bitcoin están diseñadas precisamente para funcionar sin necesidad de agente administrativo, avalista, o regulador.

¿Qué clase de sitio web debe diseñar para acceso de los interesados?

Dependiendo de la capacitación tecnológica de los diferentes grupos de usuarios de interés, las plataformas online que quieran hacer uso de criptodivisas deben hacer ciertos esfuerzos (adicionales al desarrollo web habitual) en materia de aseguramiento de la usabilidad de todo lo que es la gestión de la divisa por parte de dichos usuarios. Por ejemplo, es necesario aportar funciones de seguridad de la información sobre las transacciones que se realicen.

¿Cómo es posible acceder a la adquisición de una criptomoneda? ¿Debo disponer de alguna clase de programa informático determinado?

Un usuario puede adquirir una determina criptomoneda de dos formas:

1. A través de un agente de intermediación (broker) especializado en cambio de moneda. Esta opción es análoga a la de cambio de divisas convencionales, no electrónicas, y no requiere de software especializado.
2. Accediendo a los incentivos económicos que algunas criptomonedas, como es el caso de Bitcoin, ofrecen a aquellos usuarios de su plataforma que deseen colaborar - aportando su capacidad de cómputo - en la validación de las transacciones del sistema. Esta opción requiere instalar el software de la plataforma, que convierte al usuario en un nodo de verificación.

¿Dónde se ingresa el valor en moneda legal en el acto de compra de criptomoneda?

En una cuenta bancaria convencional, gestionada por ese agente de intermediación. Como contraprestación, el adquiriente recibe una asociación de su identidad electrónica de usuario con la moneda que haya adquirido (para la cual se utiliza igualmente un identificativo electrónico, de un modo análogo a lo que en el mundo de la moneda convencional se conoce como número de serie). Esta asociación (pública) es todo lo que hace falta para representar la *propiedad* de la moneda. La privacidad del usuario se mantiene mediante el uso de criptografía de clave pública, que consigue el efecto de *desacoplar* la identidad electrónica del usuario de su identidad física. Además, como una unidad de moneda se puede dividir en partes (la *divisibilidad* es una de las propiedades "fundamentadoras" de la emisión de moneda), cada una de esas nuevas partes también se dota de su propio identificador.

¿Cómo se fija inicialmente el valor de la criptomoneda y la cantidad total de la misma? ¿Puede irse ampliando la cantidad?

Depende. Algunas criptomonedas, como es el caso de Bitcoin, Ether o Litecoin, están diseñadas con un número inicial y constante de unidades, con el objetivo de controlar la oferta. Se mantiene un importante paralelismo con el patrón

oro. No se busca representar *deuda*, como ocurre en el caso de los Bancos Centrales, sino representar a la moneda en sí misma. Por este motivo se opta por establecer un número fijo de unidades de moneda, de manera que es el *valor* de cada unidad lo que oscila, en función de la oferta y la demanda del mercado. Debido a esto no se puede *devaluar* este tipo de moneda mediante inflación, como ocurre con las monedas convencionales. Tampoco se puede *falsificar*. Por ejemplo, en el caso de Bitcoin existen 21 millones de unidades de moneda, ni una más ni una menos. Por el contrario, otras criptomonedas, como es el caso de BitShares o PeerCoin, sí contemplan mecanismos para el acuñado de nueva moneda.

¿Por qué una criptomoneda cambia de valor? ¿Dónde se puede visualizar su evolución?

Una moneda convencional cambia de valor en función de la confianza o reputación que le otorgan sus usuarios, y en función de los deseos de éstos de comprar o vender dicha moneda. En el caso de las criptomonedas, la asignación de valor funciona exactamente igual. Es posible observar la evolución del valor de una criptomoneda en las numerosas agencias de compra-venta de moneda. En el caso de Bitcoin es posible seguir su evolución en la web www.bitcoin.com.

¿Podría darse el caso de que pierda todo o mucho de su valor provocando un "crash"? ¿Habría alguna responsabilidad?

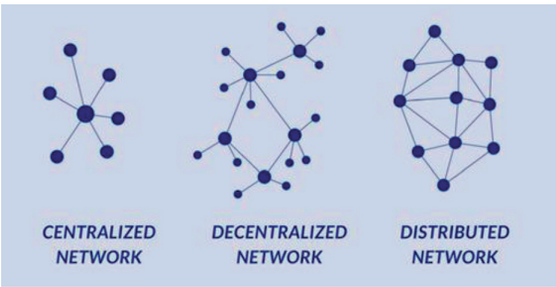
Desde luego, aunque ésta es una hipótesis que también puede darse en el caso de monedas convencionales. En el caso de monedas físicas, de curso legal, existen unas ciertas responsabilidades en la autoridad central que gestiona dicha moneda. A partir de estas responsabilidades se establecen algunos mecanismos para reducir el impacto potencial en caso de darse una situación de estrés, ante algunos supuestos concretos. Estos mecanismos no suelen ser infinitos; están sujetos a la disponibilidad de recursos y tienen un límite. Precisamente por constituirse en forma de emisión de *deuda*, las monedas convencionales pueden alcanzar un valor muy superior al que pueda existir como soporte físico de las mismas (si bien es cierto que ya no es imprescindible contar con un soporte físico, como puede ser el oro, etcétera), y esto hace imprescindibles esos límites. En el caso de las monedas digitales descentralizadas, la responsabilidad como tal no existe en el diseño, si bien siempre está la puerta abierta a que agentes con interés por la responsabilidad (social) añadan prestaciones al sistema. Los usuarios de criptomonedas también pueden ver dañado su valor en situaciones de fallo informático, virus, etc.

¿Cómo se pueden adquirir bienes o servicios con criptomonedas? ¿Quién las acepta?

Cualquier entidad mercantil puede aceptar el pago de sus productos o servicios en criptomoneda. Solamente tiene que habilitar el acceso técnico a este tipo de pago. Por ejemplo, Microsoft permite el pago con Bitcoin en su Windows Store. Bloomberg permite el acceso mediante Bitcoin a su publicación online.

¿Cuál es el proceso para vender las criptomonedas adquiridas? ¿Son fácilmente convertibles a cualquier otra moneda de curso legal?

Hay dos formas de vender criptomonedas, esto es



cambiarlas por una moneda convencional, física: en persona y online. En persona, un usuario puede simplemente hacer traslado de una moneda de su propiedad a otro usuario, mediante las diferentes técnicas que las plataformas ponen a disposición de los usuarios, como puede ser por ejemplo el escaneo de un código QR - que presenta el movimiento de moneda - mediante el móvil. Por supuesto, es requisito negociar el precio, por ejemplo, haciendo uso de índices de precios de agencias de intercambio de moneda, como CoinDesk.

Otra opción, es la venta de la criptodivisa través de las plataformas web de agencias de compra-venta de moneda, bien directamente entre usuarios (mediante plataformas como Coinbase o Bittylicious) o bien a través de intermediarios especializados, como puede ser el caso de BTC.

En todos estos casos, sería interesante contemplar los aspectos fiscales del movimiento de moneda.

¿Quiénes son y cómo se puede acceder al "trabajo" de controlador voluntario de transacciones?

Mediante la instalación del software de las diferentes plataformas, un usuario puede comenzar a participar en el proceso técnico de la misma, de un modo prácticamente transparente y sin necesidad de grandes conocimientos. Plataformas que contemplen el concepto de incentivo en su gestión asignan ciertas cantidades de moneda a sus usuarios colaboradores.

¿Deben disponer de conocimientos, equipos y/o metodología predeterminada?

No se requieren equipamientos costosos, ni grandes conocimientos técnicos. Tampoco metodológicos. La validación de transacciones se realiza de un modo completamente transparente al usuario. Lo que esencialmente un usuario aporta al sistema descentralizado de verificación de transacciones - y por lo que recibe incentivo a cambio, por ejemplo, en Bitcoin - es la capacidad de cómputo de su equipo e indirectamente la energía eléctrica.

¿Tienen los países (España) reglas fiscales para la adquisición, venta y/o posesión de criptomonedas? ¿Se pagan impuestos de algún tipo?

Como cualquier otro activo, una criptomoneda está sujeta a los diferentes impuestos a la renta que puedan existir actualmente en las diferentes legislaciones, como ganancia o pérdida patrimonial, en el momento de la venta. Aunque no abundan los pronunciamientos jurídicos sobre la materia, algunos expertos consideran que ya existe suficiente jurisprudencia. En particular, existe una sentencia tanto de la Dirección General de Tributos del Ministerio de Hacienda, como del Tribunal de Justicia de la Unión Europea, que considera a las transacciones en Bitcoin como transacciones financieras.

APLICACIÓN INDUSTRIAL

¿Cuáles serían los primeros pasos prácticos de una empresa industrial para comenzar la aplicación de BLOCKCHAIN?

Lo primero que necesita saber una empresa industrial es si realmente necesita hacer uso de tecnología de verificación descentralizada - como es el BlockChain, infraestructura de Bitcoin - o no. En general, este tipo de infraestructura adquiere su valor y puede proyectar un salto cualitativo en aquellas situaciones en las que múltiples agentes tienen que realizar gestiones particulares pero dependientes unas de otras sobre un determinado activo. Un ejemplo paradigmático es el de diferentes empresas industriales que deben realizar transformaciones particulares secuencialmente sobre un cierto producto en transformación. Así, la trazabilidad -uno de los grandes retos de la industria - tiene en las tecnologías descentralizadas un razonable aliado de futuro.

Descontado este primer ejercicio de reflexión y búsqueda de sentido, ante un reto industrial realmente distribuido, el siguiente paso no es otro que el de dotarse de infraestructura especializada (muy probablemente en asistencia por parte de una consultoría), prueba de la consistencia de la misma y validación de sus funciones principales y puesta en explotación. Es importante hacer especial énfasis en que, dado que serán varios los agentes industriales que entren en juego, todo el despliegue técnico debe hacerse en colaboración y con integración.

En principio se supone que es para la gestión segura de la información ¿En qué procesos o sistemas tendría sentido implementarla? ¿En qué tipo de transacciones aparte de las financieras tendría utilidad?

Sistemas como BlockChain no aportan seguridad por sí mismos. Su función es la de la verificación descentralizada de transacciones, a salvo de agentes centrales sobre los que no se desea depositar la confianza. La seguridad de la información debe añadirse *además* de esto. Tiene sentido utilizar esta tecnología en escenarios en los que diferentes entidades realizan procesos particulares sobre un mismo activo.

Puede tener una gran utilidad en el reto de dotar de consistencia a la información provista por sistemas de IoT (Internet of Things) Industrial, en los que colecciones de sensores o dispositivos distribuidos (a menudo también heterogéneos) proveen información que debe cohesionarse. Una plataforma BlockChain especializada en el dominio de IoT es IOTA.

¿Tendría sentido en una empresa o fábrica unitaria? ¿Sería más propio para multinacionales o empresas con diferentes sedes, ramas o negocios?

En el caso de una única empresa (o también de una célula de proceso) que tiene toda la información que requiere para llevar a cabo su función, tecnologías como BlockChain no aportan mucho más que una base de datos convencional. Cobra su sentido cuando son diversos los actores en juego.

¿Se podría aportar un ejemplo muy sencillo de cuál sería la información a transmitir? ¿Quiénes son los diferentes actores, etc.?

En materia de trazabilidad de plataformas industriales (como utillajes u otros), BlockChain supone un ejemplo paradigmático de lo que podría conseguirse, en el objetivo de dar una única visión cohesionada, consistente, de toda la información que ha pasado por dicha plataforma a lo largo de su recorrido a través de las diferentes empresas transformadoras.

En definitiva, sobre todo en escenarios de cadena de suministro, logística, trazabilidad, etc., BlockChain está llamado a proporcionar al sector industrial grandes beneficios, en su aplicación cualquier problema descentralizado, en el que entren en juego varias partes que requieran verificar su aportación al conjunto y aportar información confiable a los siguientes actores de la cadena.

eit InnoEnergy
Knowledge Innovation Community

InnoEnergy **Master's School**

Ingenieros de hoy. Innovadores del mañana.

Toma tu lugar en el futuro energético.
¡Inscríbete hoy!

7 programas de máster

14 universidades europeas

10 países

3 escuelas de negocio

70+ socios industriales

27 nacionalidades

1 comunidad pan-Europea

Doble diplomatura:
2 años
2 universidades

93% de estudiantes
con puestos de trabajo relevantes
6 meses después de la graduación

15% por encima del salario medio europeo

12% de graduados
crean sus start-ups después de la graduación

Inscripciones abiertas hasta el 22 de abril de 2018

Más información e inscripción
www.innoenergy.com/masterschool
Contacto: **masterschool@innoenergy.com**

www.innoenergy.com

InnoEnergy is supported by the EIT, a body of the European Union