3.- Comisión de Asuntos Económicos y Monetarios

Las Bitcoin y la Ingeniería Económica. Criptomonedas o Tecnología Blockchain

Introducción

Como sucede, desde que la informática existe en la vida del ser humano, se van produciendo **avances** de manera continua. Uno de los últimos ha sido la creación e implantación de la **cadena de bloques** o **blockchain** y como consecuencia la creación de las criptomonedas.

Fruto de la iniciativa de unos programadores, que en los años 90 definen una solución para la realización de **pagos electrónicos**, nace la cadena de bloques o blockchain. Esta tecnología, que serviría en aquel entonces para **crear monedas electrónicas** y para **otras funciones**, es en la actualidad soporte de muchos proyectos de innovación tecnológica así como generadora de economía basada en la moneda electrónica.

La cadena de bloques o blockchain es un avance reconocido mundialmente como la **quinta evolución de la informática**.

Esta revolución se traduce a nivel mundial en un posible cambio de la economía, en donde las monedas no dependerán de entidades nacionales como los bancos y pasarán a ser un elemento público, en el caso de iniciativas populares o un elemento en manos de las entidades privadas como las grandes empresas.

Blockchain

La cadena de bloques es una tecnología que se basa en tres pilares.

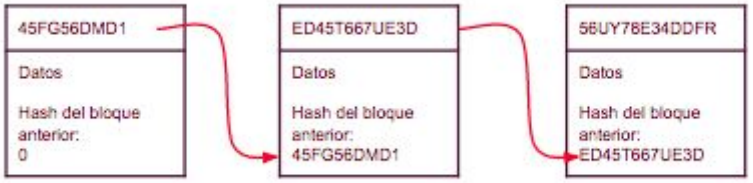
- Unas estructuras de datos organizada en unidades llamada **bloques**.
- La encriptación de los **enlaces** de la cadena para que no pueda ser descifrada y cambiada.
- Una red de **nodos** que se encargan de la gestión, creación y validación de la estructura de los datos.
- **Minería** es la actividad realizada por cada nodo que deriva en el pago por parte del blockchain en moneda del mismo al nodo que trabaja para la blockchain.

Estos tres pilares son soportados por **programas informáticos** que, en cada uno de ellos, cubren todas las funcionalidades requeridas.

¿Para qué sirve cada una de las partes de la cadena de bloques o blockchain?

- **Bloque**: es el componente que guarda los **datos asociados a una transacción** de criptomoneda, relativa a un **contrato inteligente** o a **otro tipo de datos** que se puedan guardar en formato electrónico.

  Cada uno de los bloques **contiene información del bloque anterior,** de manera que esta información también forma parte del bloque. Está peculiaridad permite que no se pueda cambiar el contenido de un bloque sin alterar la cadena por completo.



Los datos que se almacenan en cada bloque pueden ser de diversa naturaleza. En el entorno de las monedas virtuales o criptomonedas sirven para indicar quién es el **poseedor** de una de ellas, en entornos Ethereum sirven para que las partes que quieran **firmen acuerdos** a través de **contratos inteligentes (smart contracts)**. Cualquier dato que quede registrado en el bloque podrá ser consultado por los usuarios, gracias a la **criptografía asimétrica**.

- **Cadena** o enlace: es un **hash** o codificación generada por criptografía que **une dos bloques** y que es creado a partir de los datos que están contenidos en el bloque anterior. De esta forma el código es único y significa una **huella digital** de estos datos, bloqueándolos en el **tiempo** y en la **posición** del bloque.

  Cada hash se crea de una información de inicio que será el **contenido del bloque anterior** excepto el primero de la cadena que es creado sin esa característica. Estos hash son creados por **programas criptográficos** que consumen mucho tiempo de ejecución pues necesitan realizar **muchas operaciones matemáticas**. La idea entonces es que los nodos ayuden a crear estos hash y consigan una recompensa, en modo de monedas generalmente, para que sigan ayudando a su generación.

  Tal es la potencia y tiempo usado en la generación de hash por los nodos que para poder conocer la información de partida partiendo del hash, un solo ordenador estaría años haciendo cálculos y no lo conseguiría.

  La **modificación** de cualquiera de los **bloques** que conforman la cadena revelaría que la información **no es correcta** por lo que se deben rechazar los nodos que soportan la cadena modificada.

- **Red de nodos**: está formada por la red de ordenadores que contienen una **copia del blockchain**, **aprueban transacciones de moneda o smart contracts** y las **registran** en la cadena.
  La red que forman los nodos o equipos que trabajan para la cadena se basa en **tecnología P2P (Peer to Peer)**, que es una red en donde no hay servidores y todos los equipos funcionan como iguales.

  Está red sirve para que los nodos que crean los bloques y los validan **colaboren** entre sí **intercambiando** la información necesaria. El proceso por el cual se validan los bloques se llama **POW (Proof-Of-Work)** y se basa en la validación del bloque por parte de los nodos que están trabajando en la red P2P.

- **Minería**: la cadena de bloques o Blockchain es una **red descentralizada y distribuida**, de manera que el trabajo a realizar para cualquier dispositivo que se conecte a esta red consistirá en **procesar las transacciones**. La minería es el

centro del sistema que se encarga además de confeccionar los códigos hash a través de cálculos muy complejos. De esta forma cuantos más mineros están trabajando para su cálculo más difícil será corromper el bloque y por lo tanto más seguro será. Es por eso que el trabajo de minero **se suele pagar con la moneda del Blockchain**.

Bitcoin y otras criptomonedas

Las **generación y control** de las criptomonedas son las funciones más comunes para un Blockchain. Según el banco central europeo las criptomonedas son: "*un tipo de dinero digital no regulado, normalmente emitido y controlado por sus desarrolladores, y usado y aceptado entre los miembros de una concreta comunidad virtual*". Hay **miles de criptomonedas** actualmente, pero resaltan dos sobre las demás: **Bitcoin** y **Ethereum**.

Bitcoin es el la primera criptomoneda que creó el primer Blockchain que ha existido,

- su primera transacción se efectuó el día 3 de Enero de 2009,
- pertenece a la **primera generación** la (1.0) y es público,
- el hash se basa en un algoritmo llamado **Sha-256** y dispone de minería,
- su algoritmo de consenso es el proof of work (**PoW**),
- la validación de bloques es cada **10 minutos**,
- el nivel de **dificultad de la minería** se recalcula tras 2016 bloques minados,
- hay un total de **21 millones** de bitcoin totales,
- su función principal es ser una **sistema de pago** de bienes y servicios descentralizado y seguro.

Bitcoin tiene comisiones para los mineros cada vez mayores conforme va creciendo la red. Las unidades de Bitcoin tienen como máximo 8 decimales: bitcoin milibitcoin (1 mBTC = 0,001 BTC), microbitcoin (1 µBTC=0.000001 BTC) y la unidad más pequeña, el shatoshi (1 shatoshi = 0.00000001 BTC). Además los mineros reciben comisión por transacción.

Ethereum

- es una criptomoneda creada el 30 de Julio de 2014,
- pertenece a la **segunda generación de Blockchain** (2.0), su Blockchain es público,
- su hash se basa en un algoritmo "**Ethash**" y dispone también de minería como forma de creación y distribución de la moneda,
- su algoritmo de consenso es proof of work (**PoW**), actualmente se está implantando un cambio a Proof of Stake (**PoS**),
- se valida un bloque aproximadamente cada **16 segundos**,
- el nivel de dificultad es recalculado por cada bloque minado,
- hay un total de **18 millones de Ethereum por año,**
- a diferencia del Blockchain de bitcoin el de Ethereum **tiene más funciones** que la de crear criptomoneda, también es una plataforma de **Smart contracts**.

Tiene comisión para los mineros en función del trabajo realizado para verificar la transacción. En Ethereum las unidades tienen como máximo 18 decimales y sus nombres son Ether, finney, szabo, shannon, babbage, lovelaces, wei. Ether= 1000 Finney= 1000000 Szabo…Cada una es 1000 veces mayor a la siguiente.

Existen muchas más criptomonedas, tantas como iniciativas se promueven por entidades y personas, cada criptomoneda usará un tipo de blockchain que puede ser estándar como el de bitcoin o realizado a medida.

Creación de la moneda compartida o bajo entidades

La idea inicial es que la cadena de bloques es una estructura de datos que **no está centralizada** y por lo tanto su soporte se basa en la **comunidad de usuarios** que la tiene compartida en sus ordenadores. Algunos de estos usuarios, llamados **mineros**, ayudan a crear los bloques y guardarlos una vez que la comunidad los valida. Por lo tanto el blockchain, y también la moneda generada, no tiene porqué **ser privada** ni estar sujeta a ninguna entidad pues **no pertenece a nadie**, aunque dependa de que muchas personas ayuden a su mantenimiento y creación.

En sentido opuesto sí puede ocurrir que determinadas entidades como bancos, estados, **entidades privadas quieran generar criptomoneda** y pongan a disposición del blockchain los recursos adecuados para su creación y registro de transacciones. En este caso el **control** de la criptomoneda estaría **a cargo de la entidad** y sería controlada por ésta. Toda la potencia de computación que es necesaria para tener la criptomoneda es dispuesta o aportada por la entidad.

Ya hay diversos proyectos a nivel privado como la **moneda de Facebook** que está siendo apoyada por otras entidades como Uber, Spotify, Booking o Visa. En este caso serían las entidades asociadas las que darían valor a la moneda poniendo a disposición de los usuarios sus productos que lógicamente se pagarían con ella.

Como podemos ver las criptomonedas pueden **crearse sin control** (ciudadanos) o por el contrario que sean **controladas** por el responsable de su creación (empresas bancos o estados), por lo tanto se nos plantea un dilema al respecto en el cual hay que decidir sobre las consecuencias y como se puede ayudar a través de la regulación a que su uso sea correcto y no afecte a los ciudadanos.

Coste de la Minería

El uso y mantenimiento de los distintos Blockchain del mundo genera un problema, el alto **consumo de energía en el minado** de las criptomonedas y por lo tanto tiene un claro impacto ecológico en emisiones de CO_2. Esto se debe a que en algunos casos los protocolos de validación como **PoW** no son **eficientes energéticamente** ya que necesitan muchos ciclos de proceso y cálculo en los equipos.

El portal Digiconomist (Portal de análisis tecnológico en monedas digitales), estimó que el **gasto eléctrico en minería de bitcoin superó** al gasto eléctrico de países como Dinamarca, Bulgaria y Bielorrusia, y supuso más del 25% del consumo de energía de Holanda, el 15% de Australia o el 10% de Reino Unido. Por este motivo la Agencia Internacional de Energía (IEA) posiciona al Bitcoin y al resto de las criptomonedas como uno de los negocios que más electricidad consume a nivel mundial.

Nos encontramos por lo tanto que mientras que los algoritmos de consenso y el consumo de los ordenadores que trabajan en la creación de criptomonedas **no se mejoren** el

medioambiente se verá afectado si se eleva el uso de las criptomonedas como elemento de intercambio de bienes y servicios a nivel mundial.

Desde el punto de vista de la regulación se debería tener en cuenta el **tipo de Blockchain** que debería ser permitido para que el medioambiente no fuera dañado. Las pruebas de esfuerzo actuales que son: **PoW, PoS, DPoS, PoI, BFT y FBA** o las que se están creando en este momento están pensadas para minimizar el gasto de electricidad y por lo tanto aminorar el impacto medioambiental.

Uso fraudulento de las criptomonedas

Las criptomonedas están pensadas para **usarse como monedas** y por lo tanto también pueden ser usadas para **comprar o vender otras monedas**. Este hecho ha permitido en ocasiones que se pudiese comprar criptomoneda con dinero "negro" y por lo tanto "blanquear" el dinero que no estuviera registrado.

Monedas como el bitcoin, se usan para **especular y/o como inversión** y también como medio de pago. Una de sus principales características es que las **transacciones** realizadas con ellas **no están controladas** por los bancos y por lo tanto están fuera del circuito de denuncias por blanqueo.

Otro elemento que puede fomentar delitos es que el **conocimiento de las transacciones** y por lo tanto el de los **individuos que las realizan** es muy complicado debido a la encriptación que se usa en el Blockchain. Por lo tanto, todas estas circunstancias unidas a la falta de control de los bancos han supuesto que los delincuentes utilicen las criptomonedas para el blanqueo de capitales obtenidos con la comisión de delitos (tráfico de drogas o de personas, entre otros).

Conclusiones

Una vez conocidos los aspectos relacionados con el Blockchain y las criptomonedas quedan muchas preguntas que responder sobre su futuro y el entorno tecnológico y legislativo que se debe formalizar.

Cuestiones para la reflexión

- ¿Se debe regular tecnologías como Blockchain?
- ¿Se deben regular transacciones realizadas con monedas virtuales?
- ¿Deben los bancos centrales apropiarse de estas monedas para seguir controlando la economía?
- ¿Debería prohibirse el cambio de monedas virtuales a monedas reales a fin de evitar la especulación?
- ¿El uso de la criptomoneda debería pagar impuestos para cuidar el medioambiente?
- ¿Debe la UE promover el uso de criptomoneda?
- ¿Deben usar las compañías su propia criptomoneda?
- ¿Los ciudadanos deberíamos crear nuestra propia moneda?
- ¿Debe la UE fomentar el uso de Blockchain como registro seguro de datos?
- ¿Es la criptomoneda un elemento seguro para los ciudadanos?
- ¿Podría ser la tecnología Blockchain una herramienta de libertad para los ciudadanos?

- ¿Es posible un mundo mejor si usamos las criptomonedas?

Fuentes:

- Blockchain For Dummies®, Published by: John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774
- The Science of the Blockchain Roger Wattenhofer, Inverted Forest Publishing
- "Blockchain Revolution" Tapscott, Don. "Penguin Random House LLC 375 Hudson Street New York, New York 10014"
- Bitcoin: conceptos, tecnología y usos https://learn.unimooc.com/student/courses/course?course=bitcoin;utm_source=desktop&utm_medium=txt
- Ethereum https://es.wikipedia.org/wiki/Ethereum
- Blockchain https://es.wikipedia.org/wiki/Cadena_de_bloques
- Algoritmos de consenso https://criptotario.com/que-es-un-algoritmo-de-consenso-en-blockchain
- Blanqueo de Capitales https://ilia.cat/blog-ilia-consultoria/criptomonedas-blanqueo-capitales/
- BlocKchain el libro https://libroblockchain.com/
- Preguntas frecuentes sobre Bitcoin https://www.criptonoticias.com/educacion/20-preguntas-frecuentes-bitcoin-blockchain-criptomonedas-parte-1/
- Criptomoneda de FaceBook https://elceo.com/tecnologia/libra-de-facebook-sera-la-kryptonita-de-los-bancos-en-el-futuro/
- BitCoin https://es.wikipedia.org/wiki/Bitcoin

Contacto

El presente informe ha sido elaborado por Francisco Javier Cárceles Moreno.
Ingeniero Técnico en Informática de Gestión en la Escuela Universitaria de Informática de la UPM.
Se pueden plantear preguntas sobre el tema en la dirección de correo electrónico:
fco.javier.carceles.moreno@gmail.com