ECONOMÍA DIGITAL: BITCOINS

Pablo Pérez Jiménez

1. Introducción

La primera especificación del protocolo Bitcoin fue publicada en 2009 por Satoshi Nakamoto, el cual abandonó el proyecto en 2010, a partir de ese momento, la comunidad Bitcoin ha crecido exponencialmente. El protocolo Bitcoin y su software son públicos y cualquiera puede revisarlo o crear su propia versión del software.

La idea de original de bitcoin era crear una moneda completamente independiente de cualquier autoridad, descentralizada, que se pudiera transferir inmediatamente de forma electrónica y con costes de transacción muy bajos.

2. ¿Qué es Bitcoin?

Bitcoin es una criptodivisa, una moneda virtual e intangible. Sus principales características son:

- **Descentralizada:** No es controlada por ningún estado, banco o empresa. No es posible generar inflación al crear más moneda, sino que la propia red gestiona de forma descentralizada en función de la demanda real la emisión de los bitcoins. Al tratarse de un servicio P2P (*peer to peer),* no tiene un servidor propio, sino que usa una red de servidores.
- **Imposible su falsificación o duplicación:** Un sofisticado sistema criptográfico protege a los usuarios y simplifica las transacciones. Cada usuario cuenta con su propio monedero.
- **No hay intermediarios:** Transacciones directas de persona a persona. Su funcionamiento P2P permite transacciones casi instantáneas.
- **Transacciones irreversibles:** Una vez realizado el pago, no se puede anular la transacción, ya que al no existir intermediario, las devoluciones dependen completamente del acuerdo entre ambas partes.
- **Privacidad:** Esta es una de las principales características que inspiró la creación, ya que no es necesario revelar tu identidad para hacer negocios.
- **Disponibilidad:** El dinero te pertenece al 100%, no puede ser intervenido por nadie, ni las cuentas pueden ser congeladas.

3. Blockchain (Cadena de bloques)

Bitcoin se basa en una contabilidad pública llamada *"Blockchain"*, considerada la mayor innovación tecnológica de bitcoin, ya que esta contabilidad contiene cada transacción procesada a través de la red. La *blockchain* es una base de datos de transacciones en la red compartida por todos los ordenadores que participan del protocolo Bitcoin, esta base de datos mantiene una creciente lista de registros de todas las transacciones.

Cada bloque dentro de la *blockchain* contiene un *hash* del bloque anterior, esto tiene el efecto de crear una cadena de bloques, desde el bloque génesis (inicial) al bloque actual. Cada bloque está garantizado para llegar después del bloque anterior, ya que de no cumplirse, el hash del bloque anterior no se conocería. Una vez el bloque lleva un tiempo en la cadena, es computacionalmente inviable modificarlo, ya que si lo modificáramos, deberíamos modificar dicho bloque y todos los bloques generados después de él. Gracias a estas propiedades, la posibilidad del doble gasto de bitcoins se vuelve muy complicada.

Basada en el protocolo Bitcoin, la base de datos de *blockchain* esta compartida por todos los nodos participantes. La copia completa de la *blockchain* contiene registros de todas las transacciones realizadas desde el origen hasta la actualidad. No obstante, el continuo crecimiento de la *blockchain* supone un problema de almacenamiento y sincronización, ya que, cada 10 minutos un nuevo bloque es añadido a la *blockchain*.

4. ¿Cómo funciona?

Para comenzar a usar el protocolo Bitcoin y realizar operaciones, es necesario instalar en el ordenador o móvil una cartera virtual, esta cartera genera una dirección única, que nos servirá para hacer o recibir transacciones. Cada cartera virtual tiene una llave privada que se utiliza para verificar nuestra identidad al hacer transacciones.

Las transacciones con bitcoins se verifican al añadirse a la *blockchain*, una cadena de bloques que mantiene un registro de todas las transacciones que se realizan en la red, además, la *blockchain* se encarga de asegurarse que un usuario tiene en su cartera los bitcoins que pretende gastarse en la transacción. En definitiva, una transacción es una transferencia entre dos carteras virtuales de bitcoins, estas transacciones son transmitidas y confirmadas en la red mediante el proceso de minería.

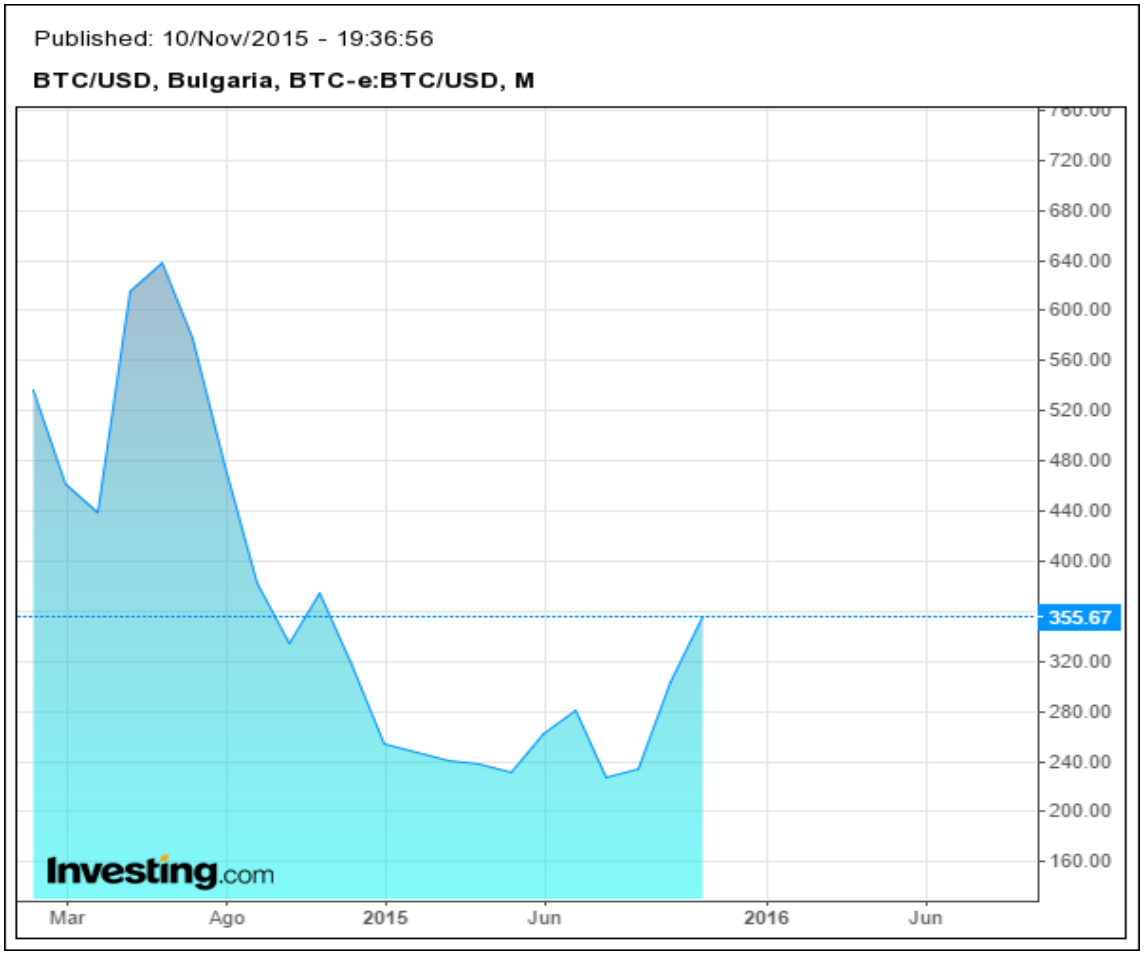
La minería es un sistema distribuido que se encarga de confirmar e incluir cronológicamente transacciones en la cadena de bloques. Para evitar que la red se inunde con nuevos bloques de cada minero, todos igualmente válidos, se obliga a los ordenadores a realizar cálculos en principio inútiles, pero que servirán para comprobar

que el ordenador ha estado trabajando alrededor de 10 minutos. La mayor parte de las veces los mineros no consiguen resolver los cálculos a tiempo y tienen que aceptar el bloque creado por otro minero, en el caso de tener éxito, tienen un buen incentivo, ya que reciben 25 bitcoins.

Cada 10 minutos, un minero crea un nuevo bloque de la *blockchain* y se generan bitcoins como recompensa. Actualmente, el número de bitcoins generados por bloque es de 25, cada cuatro años esta recompensa se reduce un 50%, hasta alcanzar un máximo de 21 millones de bitcoins generados. Se calcula que el último bitcoin será generado en Mayo de 2140.

5. ¿Cuánto vale un Bitcoin?

El valor del bitcoin se basa en la oferta y la demanda, y se calcula mediante un algoritmo que mide la cantidad de movimientos y transacciones con bitcoin en tiempo real. Bitcoin está catalogada como la moneda más inestable del mercado de divisas, como podemos ver en la gráfica, en Junio de 2014 su valor rondaba los 640$/Bitcoin y en solo un año perdió casi 400$ de valor situándose cerca de los 240$/Bitcoin.



6. Bibliografía

[Gráfica Valor Bitcoins]: http://es.investing.com/currencies/btc-usd-chart

[Wiki Bitcoins]: https://es.bitcoin.it/wiki/P%C3%A1gina_principal

[Páginas de Interés]:

https://bitcoin.org/es/

http://computerhoy.com/noticias/internet/que-es-bitcoin-como-funciona-donde-compran-5389

https://en.wikipedia.org/wiki/Bitcoin

https://www.weusecoins.com/

http://elpais.com/tag/bitcoin/a/

http://money.cnn.com/infographic/technology/what-is-bitcoin/