Criptomonedas: Bitcoin y su funcionamiento

Con el nacimiento en 2009 de Bitcoincomenzó la carrera de las criptomonedas que aún no sabemos muy bien hacia donde se dirige, puede que terminen por implantarse como un medio de pago o por el contrario pueden fracasardesapareciendo y dejándonos interesantes tecnologías como Blockchain.

Recientemente han vuelto a aparecer en las noticias por la fuerte caída que han sufrido en el último mes, especialmente elBitcoin.

Estas criptomonedas utilizan blockchain (sistema de base de datos distribuido) para funcionar, de esta manera no es necesaria la utilización de intermediarios en la emisión de transferencias. En nuestro sistema financiero actual, el intermediario normalmente es un banco que se encarga de verificar la confidencialidad e integridad de la transferencia entre dos participantes. En bitcoin no existen intermediarios, las transferencias se realizan y son verificadas por los distintos nodos que componen la red.

Para verificar la seguridad de las transferencias y evitar que el dinero se utilice en repetidas ocasiones se utiliza una cadena de bloques. Los hashes de las transacciones quedan reflejados en esta cadena basada en una prueba de trabajo, de esta manera las transacciones quedanalmacenadas y no se pueden modificar sin superar la prueba de trabajo. Esta cadena de bloques contiene toda la secuencia de eventos de bitcoin desde su comienzo.

Al funcionar bitcoin mediante un sistema de comunicaciones de nodos distribuido, como lo es una red peer to peer, la integridad de la cadena de bloques no estará comprometida mientras la mayoría del poder computacional (que manejan dichos nodos) se encuentre en nodos que cooperen con el sistema de forma honesta.

Para esto el sistema cuenta con distintos incentivos que hacen más interesante para los atacantes cooperar con el sistema que atacarlo para obtener un beneficio, aunque hay que decir que estos incentivos podrían no funcionar ante posibles ataques motivados por otra causa que no sea la económica.

El sistema de comunicaciones que utiliza bitcoin es robusto gracias a su simplicidad, los nodos trabajan conjuntamente con una mínima coordinación.Estos pueden abandonar la red cuando deseen, pudiendo acceder más tarde tras sincronizarse con la cadena de bloques. Cada nodo vota con su poder computacional, expresando la aceptación de los nuevos bloques (transacciones) validos o rechazándolos.

En cuanto a la privacidad, en bitcoin las transferencias entre las distintas direcciones son públicas y se puede consultar mediante la cadena de bloques. Pero no es trivial asociar una dirección a una determinada persona física. Las direcciones de un monedero pueden cambiar en las distintas transferencias, y se pueden utilizar distintos métodos como la red anónima

TOR para conseguir mantener esta privacidad entre el monedero de bitcoiny la persona física propietaria de dicho monedero.

Aparte de bitcoin existen cientos de criptomonedas como por ejemploEthereum, Ripple, Litecoin, Dash, etc.

Estas criptomonedas están siendo utilizadas actualmente para diversos fines tanto lícitos como en la mayoría de las ocasiones ilícitos por su complicada trazabilidad, que permite a delincuentes blanquear capitales, realizar compras ilegales en internet o invertir como un tipo de valor.

Borja Rodrigo

CibersecurityDepartament

Áudea Seguridad de la Información