

Cómo funciona el bitcoin, transacciones, registro, seguridad

Cómo funciona el bitcoin, transacciones, registro, seguridad. Nos interesa, no solo como tema de actualidad sino como un tema tecnológico hablar de las criptomonedas.

Control

El principal problema con las **transacciones en línea** es que los **registros digitales** se pueden **manipular** para que alguien pueda, con el tipo de interferencia correcto, gastar el mismo dinero dos veces.

Con sistemas como PayPal y Paytm, la compañía actúa como una autoridad confiable central para autenticar cada transacción.

Blockchain libro central

Bitcoin en cambio usa algo llamado blockchain para mantener registros. El blockchain es un libro público de todas las transacciones de Bitcoin que se haya realizado, y se distribuye a todas las máquinas conectadas a la red de Bitcoin. Este blockchain existirá para siempre y es imposible de editar por una sola persona. En cambio, cuando se lleva a cabo una transacción, las **computadoras de la red verifican** automáticamente los saldos de las direcciones de Bitcoin implicadas y editan el libro mayor.

Cada diez minutos, se crea un nuevo «bloque» a medida que se extraen los bitcoins (lo abordaremos un poco).



Estos 'mineros' confirman todas las transacciones desde que se

agregó el último bloque, antes de agregar el nuevo bloque a la cadena y redistribuirlo. De esta manera, nadie puede robar Bitcoins, o forjarlos de la nada simplemente cambiando unos pocos números. En lugar de una figura del **banco central**, todos tienen registros, que luego se pueden cotejar para identificar pagos fraudulentos. También significa que los pagos no son reversibles, como con PayPal, y sus cuentas nunca se pueden congelar.



Tomada de internet

Expresado de otra forma para tratar de clarificar al máximo los conceptos, de hallar mayor comprensión: Bitcoin utiliza la **criptografía de clave pública**, la red de igual a igual y la prueba de trabajo para procesar y verificar los pagos. Los bitcoins se envían (o se vuelven a iniciar) de una dirección a otra, y cada usuario puede tener muchas, muchas direcciones. Cada transacción de pago se transmite a la red y se incluye en el blockchain para que los bitcoins incluidos no puedan gastarse dos veces. Después de una hora o dos, cada transacción se bloquea en el tiempo por la cantidad masiva de **potencia de procesamiento** que continúa extendiendo la cadena de bloques. Usando estas técnicas, Bitcoin proporciona una red de pago rápida y extremadamente confiable que cualquiera puede usar.

Para quien desee documentarse un poco más al respecto, lo invitamos a leer: [Bitcoin, lo bueno, lo malo y lo feo](#); [Qué es el bitcoin](#); [seis sitios para comprar y vender bitcoins](#)