



curso de introducción al

mundo de las criptomonedas





CRIPTOMONEDAS

¿QUÉ SON Y CÓMO FUNCIONAN?

DEFINICION DE CRIPTOMONEDA

Una Criptomoneda:

- Es una moneda virtual
 - No es de curso legal
- Es convertible
 - A otras monedas digitales diferentes
- Es descentralizada
 - No controlada por un banco o ente financiero
- Utiliza tecnología digital particular:
 - Criptografía digital
 - Un sistema de libro contable distribuido (*Blockchain*)
 - Una red de computadores distribuidos

Clasificación de la moneda digital



EVOLUCION DEL DINERO



CARACTERISTICAS DE LAS CRIPTOMONEDAS



Criptografía: Utilizan técnicas de cifrado para realizar cobros y pagos seguros.



Descentralización: No necesitan ser controladas por ninguna institución.



Unico: Un sistema criptográfico protege a los usuarios de la falsificación



No hay intermediarios: Contacto directo persona a persona.



Las transacciones son irreversibles: Una vez se efectúe el pago, no hay posibilidad de cancelación.



Intercambiable: se puede cambiar por otras divisas.



Privacidad de uso: No es necesario revelar tu identidad al hacer negocios.

CARACTERISTICAS DE LAS CRIPTOMONEDAS

CENTRALIZADO



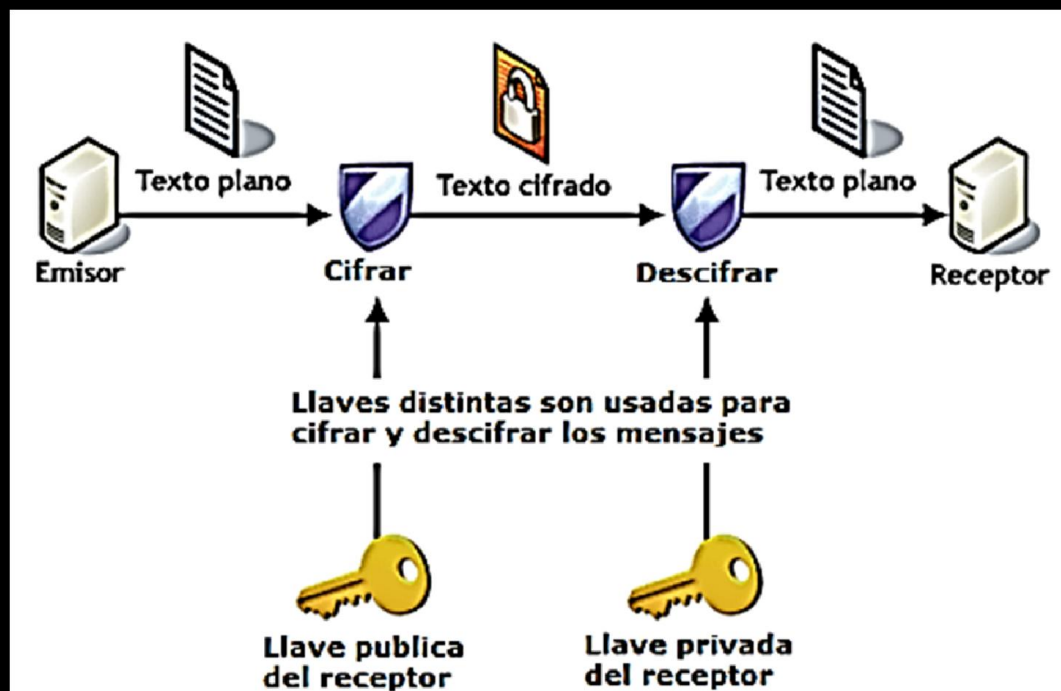
SERVIDOR
CENTRAL

DESCENTRALIZADO



NODOS

CRIPTOGRAFIA



Utiliza algoritmos matemáticos y tecnología informática para cifrar y descifrar datos o para garantizar la integridad y autenticidad de la información.

Básicamente un texto sin formato se somete a un proceso de encriptación que lo convierte en un texto cifrado (que es ilegible). Al hacer esto, se puede garantizar que la información enviada solo pueda ser leída por una persona que posea una clave de descifrado específica .

CRIPTOMONEDAS

VENTAJAS Y DESVENTAJAS

Ventajas

- **Ausencia de fronteras**, lo que facilita los **pagos**, puede favorecer al **comercio** y al flujo de **capitales**
- **Seguridad y anonimato** de las transacciones
- La **innovación** que aportan al dinero
- La capacidad de realizar **contratos inteligentes** que se ejecutan por sí mismos
- La **transparencia** en la oferta de monedas

Desventajas

- Comportamiento **volátil**, por su oferta inelástica
- **Manipulación** que pueden realizar gobiernos o mineros
- La **dificultad y el costo** asociado a las transacciones
- El **impacto ambiental** negativo por la fuerte demanda de energía
- El potencial para **actividades ilegales** dada la falta de regulación

BITCOIN



BITCOIN

El origen del Bitcoin se remonta al año **2009** y la historia señala que su creador operaba bajo el pseudónimo de **Satoshi Nakamoto**

El dominio **bitcoin.org** se registró en el año **2008** y en octubre de ese mismo año, Satoshi Nakamoto escribió un artículo que se titulaba «Bitcoin: Un sistema de efectivo electrónico entre iguales».

Bitcoin usa tecnología peer-to-peer **P2P** para operar sin una autoridad central o bancos; la gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red.



BITCOIN

PRINCIPIOS FUNDAMENTALES

Límite de 21 millones: Solo existiran 21 millones de bitcoins. Por lo tanto la oferta monetaria está **limitada**, al contrario que las monedas fiduciarias, donde el banco central puede emitir todas las que desee.

No se puede censurar: **Nadie** puede prohibir o censurar las transacciones que han sido validadas y **todos** pueden realizar transacciones sin necesidad de un permiso.

Es fungible: Todas las unidades son intercambiables.

Los pagos son irreversibles:

Las transacciones que han sido confirmadas **no pueden** ser modificadas ni eliminadas.



BITCOIN

BASES DEL FUNCIONAMIENTO

BLOCKCHAIN: Cadena de bloques de información. Es una base de datos distribuida y replicada en todos los nodos de la red

PRUEBA DE TRABAJO: PoW Resolución de un algoritmo que permite que se puedan insertar bloques en la **BLOCKCHAIN**

P2P: Procesadores conectados entre sí que permiten el intercambio directo de información de igual a igual.

Servidores descentralizados

CRIPTOGRAFIA: Tecnología para resguardar la integridad de los datos y así evitar que personas no autorizadas accedan a la información



BITCOIN REVOLUCION

POLITICA

TECNOLOGICA

FINANCIERA

SOCIAL



BITCOIN

MINERIA

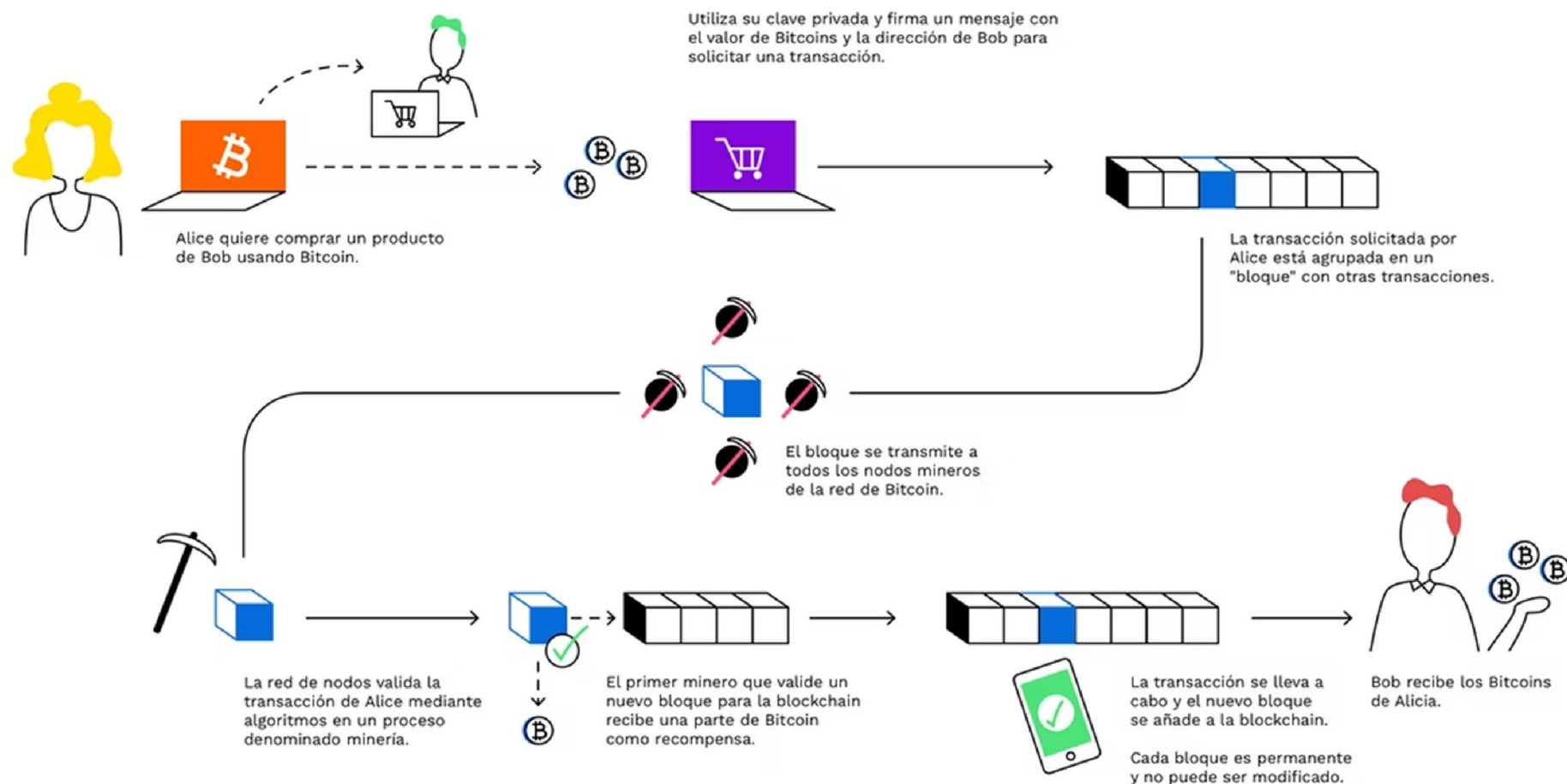


Qué es la minería de Bitcoin

cómo funciona una transacción Bitcoin

POW – PROOF OF WORK

PRUEBA DE TRABAJO

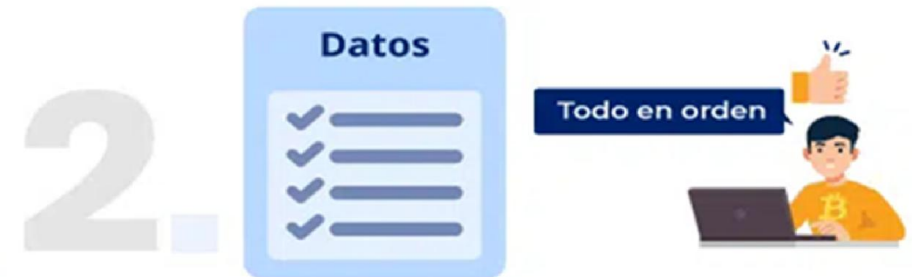


BITCOIN

MINERIA



Firmar transacciones de forma descentralizada



Verificar y registrar datos inmutables



Garantizar seguridad



Emitir nuevas monedas

BITCOIN

INCENTIVOS MINERIA

6.25 BTC: Hasta mediados del 2024

COMISIONES DE TRANSACCION

HALVING: La recompensa se reduce a la mitad cada
210.000 bloques

POOLS DE MINERIA: Para tener mas
Probabilidades de resolver un bloque



BITCOIN

HALVING



BITCOIN

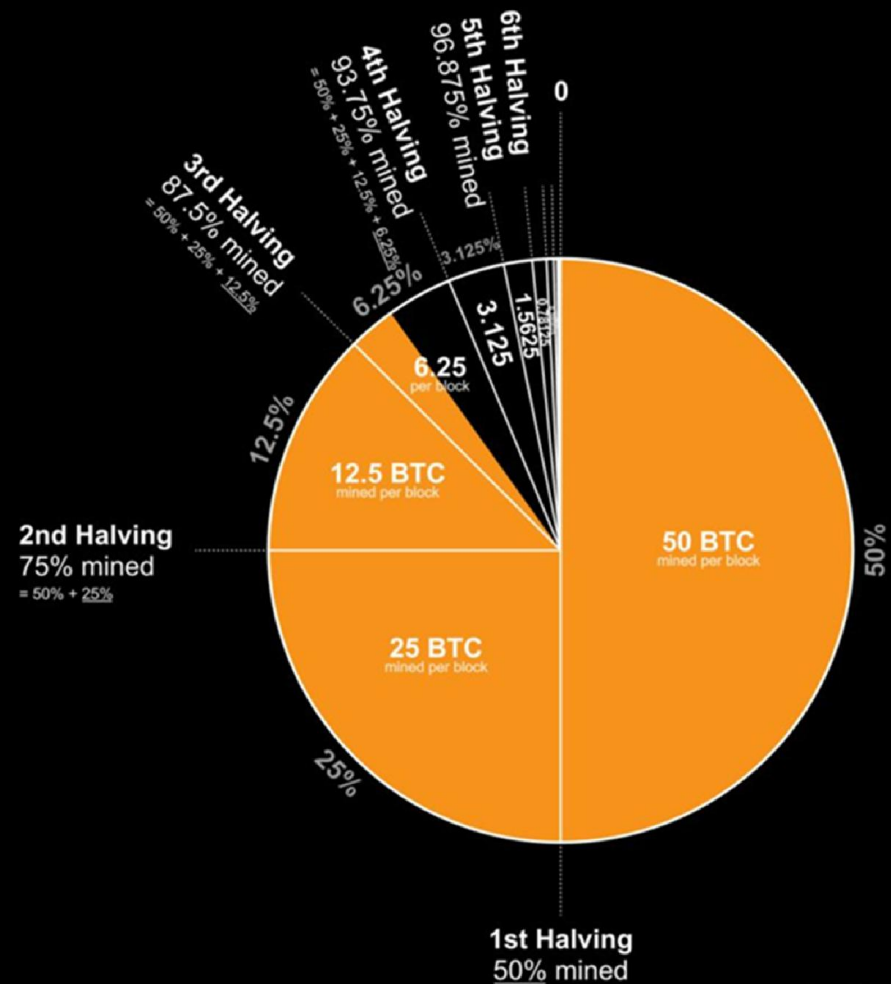
HALVING

02-03-2024: Proximo HALVING

La recompensa pasara a ser 3.125

**Cada 4 años se producira
un HALVING**

**hasta que la recompensa
sea 0,00000001 BTC
(1 SATOSHI)**



BITCOIN

HALVING

El viernes 1 de abril de 2022 a las 16:21:29, se extrajo el Bitcoin número 19 millones en el bloque 73002, lo que significa que ya solo quedan dos millones de monedas por extraer en la red, ya que no pueden haber jamás más de 21 millones de BTC en circulación.



¿cuándo se terminará de minar todo el Bitcoin que queda? Pues aunque parezca mentira, es algo que no vamos a ver en breve, ya que se espera que el último Bitcoin sea minado en el 2140, dentro de casi 120 años.

BITCOIN

EVOLUCION



BITCOIN

EVOLUCION

\$1000 EN FEBRERO 2011 = U\$S 250

SI LO GUARDASTE EN \$ HOY TENDRIAS U\$S 5

SI LO GUARDASTE EN U\$S HOY TENDRIAS U\$S 250

SI COMPRASTE 250 BITCOINS HOY TENDRIAS

U\$S 7.500.000

