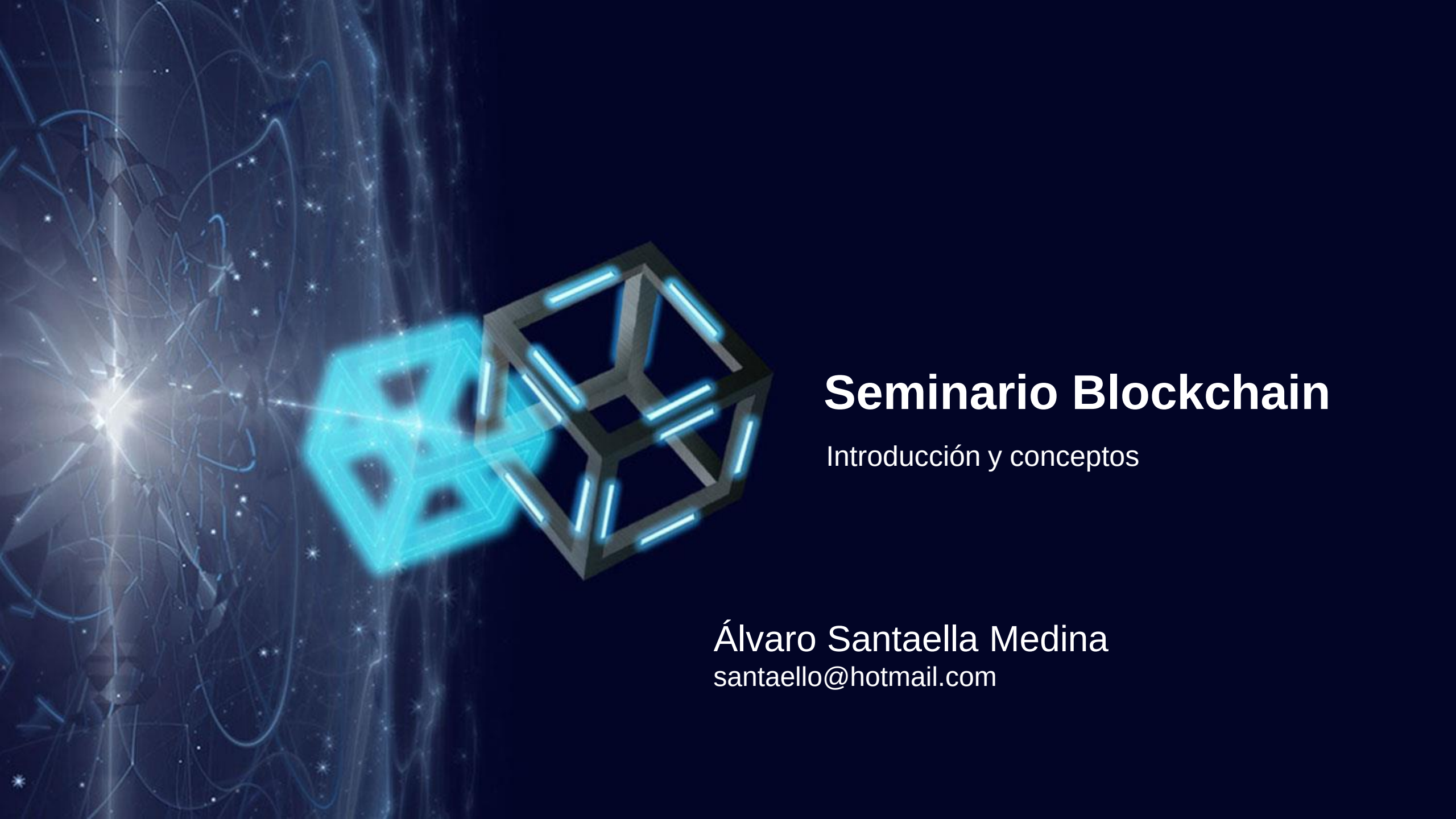
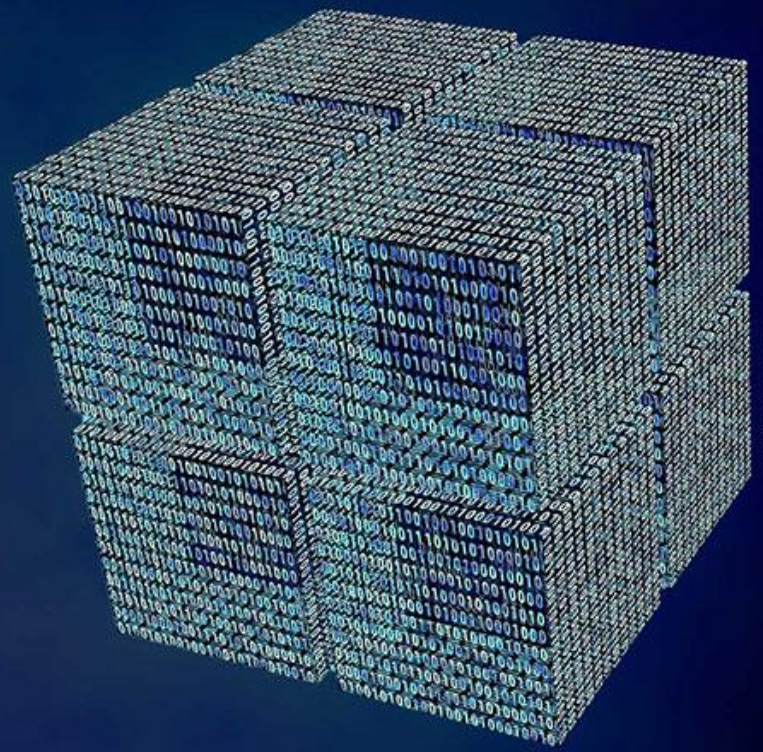


Seminario Blockchain

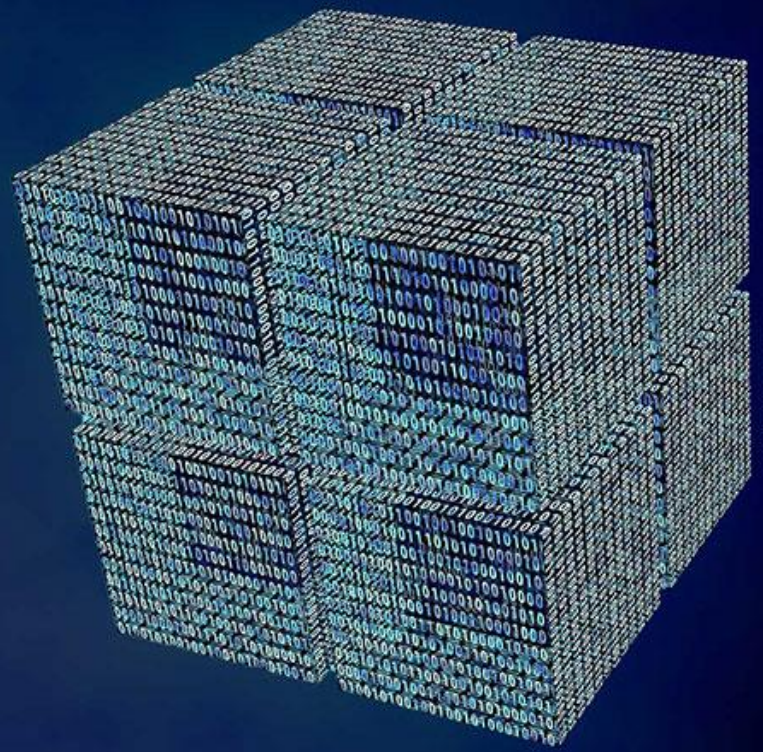
Introducción y conceptos

Álvaro Santaella Medina
santaello@hotmail.com

Agenda



- Criptografía y seguridad
- Criptomonedas y Bitcoin
- Blockchain
- Ethereum, Altcoins y Tokens
- Transacciones y Billeteras
- Exchanges
- Introducción a Defi
- NFTs y Metaverso



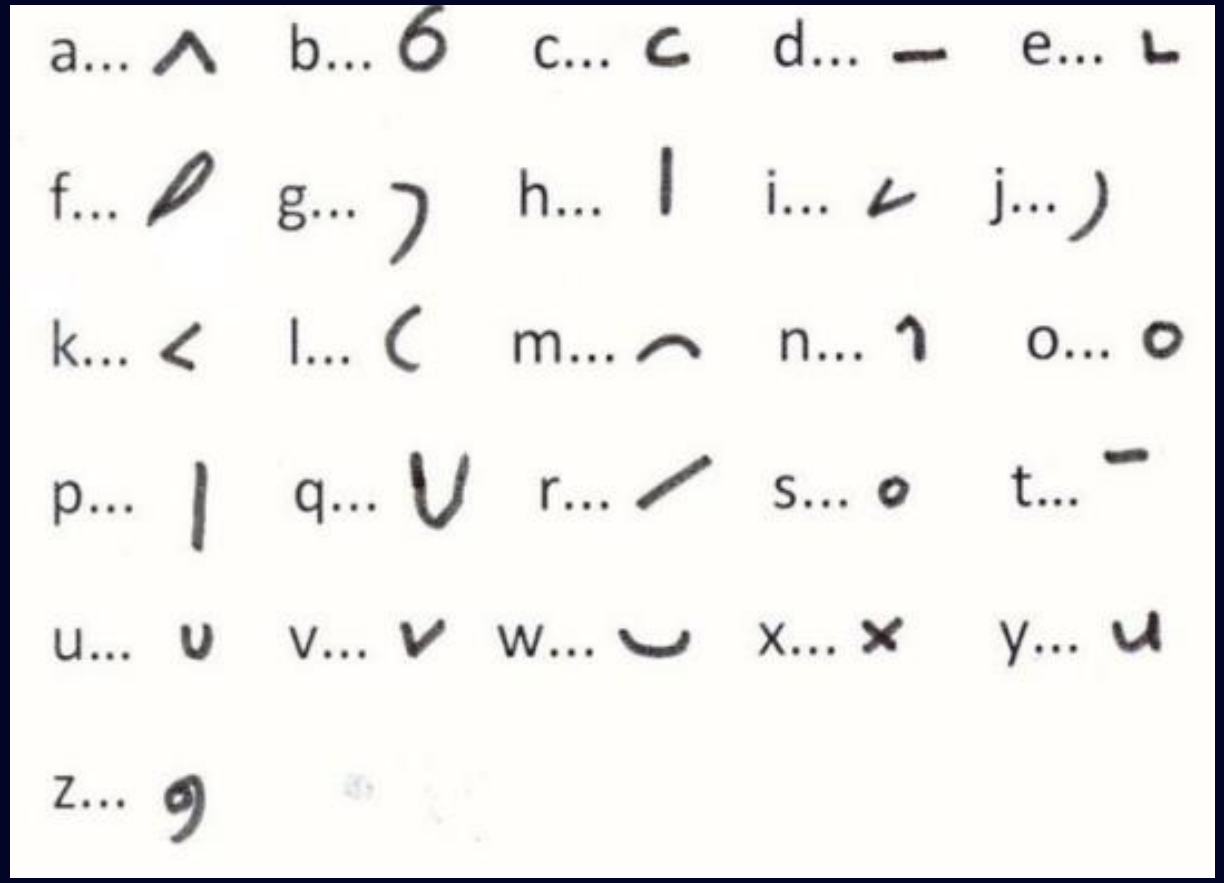
Criptografía y seguridad

Criptografia

Rama inicial de las matemáticas y en la actualidad también de la informática y la telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves

Criptografia

En sus orígenes



Criptografia

En sus orígenes…

Cifrado del Cesar

- Lo usaba Julio Cesar para comunicarse con sus generales
- Es uno de los algoritmos más sencillos de sustitución
- Se sustituye una letra por una letra 3 posiciones delante del abecedario

Criptografia

Evolución hasta hoy-…

- Sistemas electromagnéticos (principios siglo 20) → Máquina Enigma
- Primeros sistemas informáticos (años 70) → Data Encryption Standard
- Algoritmos avanzados años 2000 → Advanced Encryption Standard (AES)

Criptografia: atributos de seguridad

Confidencialidad

Que solamente tenga acceso al mensaje quien esté autorizado a su acceso

Seguridad

Integridad

Que nadie ha modificado el mensaje que ha enviado el origen

Autenticidad

Que el mensaje proviene del origen esperado

Criptografia: Autenticidad y Confidencialidad

Criptografía Asimétrica

Autenticidad

Solo quien **conoce la clave privada** puede haber cifrado el mensaje

Criptografía Asimétrica

Confidencialidad

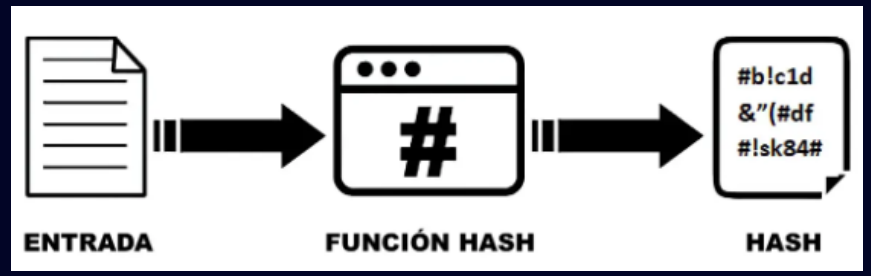
Solo quien **tiene la clave privada** puede descifrar el mensaje

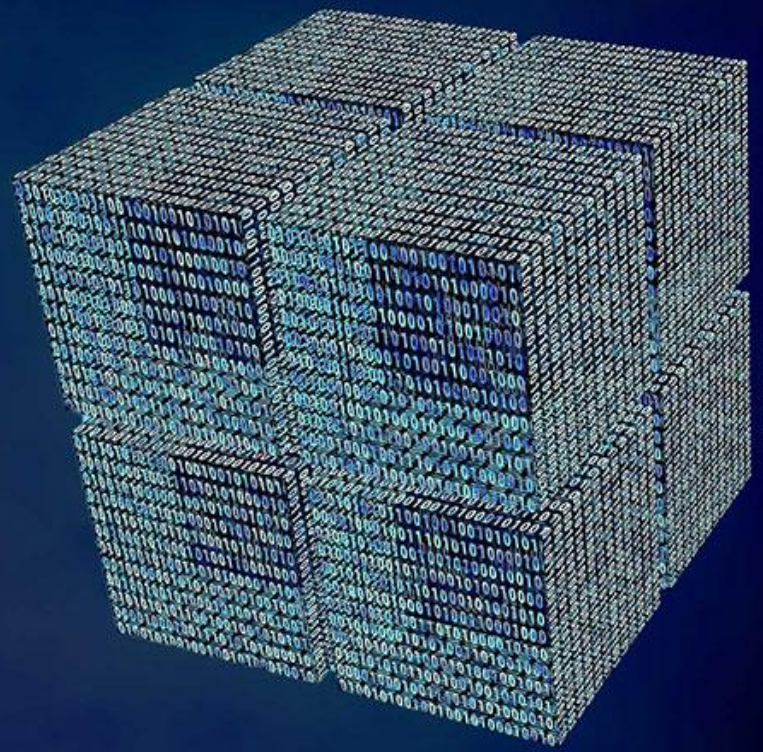
Criptografia: Integridad

Hashing → Función Hash es una función matemática que transforma cualquier elemento digital en un número máximo de caracteres

Se les llama también resumen criptográfico:

- El resultado siempre tiene el mismo tamaño
- Son fáciles y rápidos de calcular
- Imposible recalcular el mensaje original
- Dos mensajes parecidos producen dos resúmenes muy diferentes
- Muy improbable que dos mensajes produzcan el mismo resumen





Criptomomedas y Bitcoin

Qué es una criptomoneda

Una criptomoneda, criptodivisa (del inglés cryptocurrency) o criptoactivo es un medio digital de intercambio que utiliza criptografía para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido

Qué es una criptomoneda

Características principales

- Sus datos están informatizados (no existe un soporte físico).
- Sus datos están encriptados
- Comparten las características principales de la monedas tradicionales

¿Qué cualidades comparten con las monedas tradicionales?

- Funcionan como reserva de capital.
- Son divisibles o fraccionables
- Son contables
- Intercambiables mediante una transacción directa o través de un tercero
- Sirven para pagar bienes y servicios, incluso para pagar impuestos

Bitcoin

Bitcoin fue la primera moneda digital creada de una manera descentralizada. ¿Qué quiere decir descentralizada? Pues que no la controla nadie (un gobierno, banco, autoridad, empresa o grupo de personas).

Bitcoin

2008 – Se registra el primer dominio bitcoin.org. Alguien con el sobrenombre Satoshi Nakamoto publica en un foro un White Paper que explica toda la idea y forma de crear bitcoin

2009 – Entra en funcionamiento la red bitcoin

2010 – Primera transacción comercial con bitcoin. 10.000 bitcoin por 2 pizzas

2011 – Bit bitcoin llega a valer 1$. Se crean plataformas de intercambio. Bitcoin empieza a ser aceptado como forma de pago en algunas empresas

Desde entonces, el ecosistema que rodea a bitcoin no para de crecer
(nuevas ideas, nuevos proyectos, etc)

Bitcoin

Características principales

- La oferta monetaria es limitada hasta los 21 millones
- Las transacciones en Bitcoin, no se pueden prohibir ni censurar. Nadie puede dar marcha atrás ni existe alguna autoridad que pueda revocarlas
- Código abierto, cualquier persona puede leer el código, o incluso copiarlo
- Accesible para todos los usuarios con acceso a internet. Cualquier persona en cualquier parte del mundo
- No es necesario identificarse para utilizarlo
- Se puede intercambiar con cualquier moneda fiduciaria u otra criptomoneda en las diferentes casas de cambio (exchanges)

Bitcoin

Pero… ¿qué es un bitcoin? ¿Cómo y donde se guardan?

En la red bitcoin, existe un sistema de validación o de protocolo de consenso llamado “Prueba de Trabajo” o PoW (Proof of Work).

Mediante este sistema, los ordenadores / equipos conectados hacen un trabajo informático de cálculo para la resolución de un problema matemático.

Este trabajo no se hace de manera altruista. El primer ordenador / equipo que consiga resolver el problema matemático, recibe una recompensa en bitcoin y es ahí donde nuevos bitcoins se crean.

Los bitcoins no se guardan en ningún sitio. Existen porque hay un registro que así lo dice, y ese registro existe como resultado de la resolución del problema matemático.

GranadaCoin

Recompensa 100 GranadaCoin

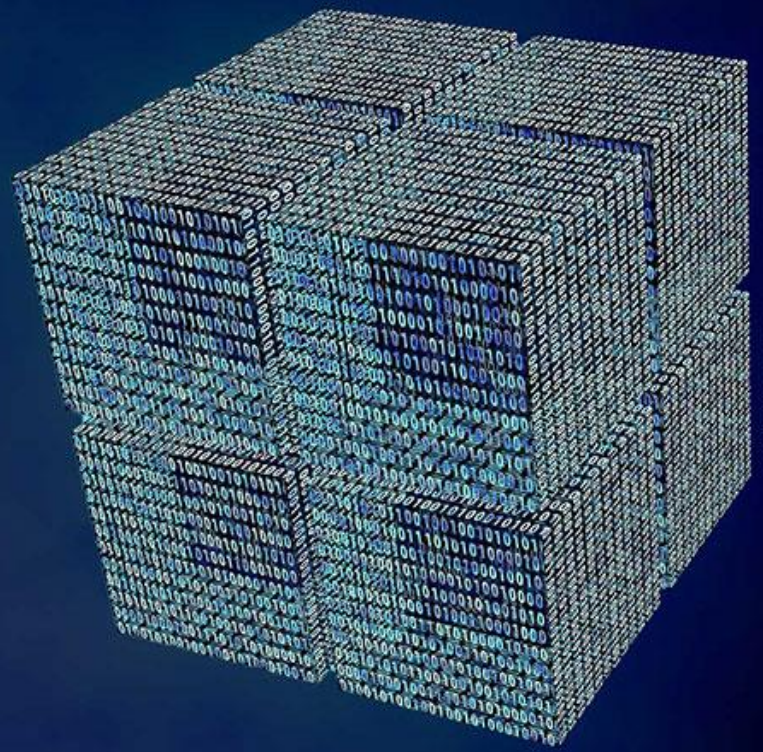
- 78 - ? – 12 = 40 — Profesor A recibe 100 — Profesor A manda 50 a profesor B
- 45 + ? + 2 = 94 — Profesor C recibe 100 — Profesor A envia 10 a Profesor D
Profesor C envia 40 a Profesor E
- 20 - ? + 2 = 12 — Profesor A recibe 100

Bloque	Transacciones	Problema	Libro Mayor
1	----------	78 - ? – 12 = 40	Profesor A recibe 100
2	Profesor A envia 50 a Profesor B	45 + ? + 2 = 94	Profesor A envia 50 a Profesor B Profesor C recibe 100
3	Profesor A envia 10 a Profesor D Profesor C envia 40 a Profesor E	20 - ? + 2 = 12	Profesor A envia 10 a Profesor D Profesor C envia 40 a Profesor E Profesor A recibe 100

GranadaCoin

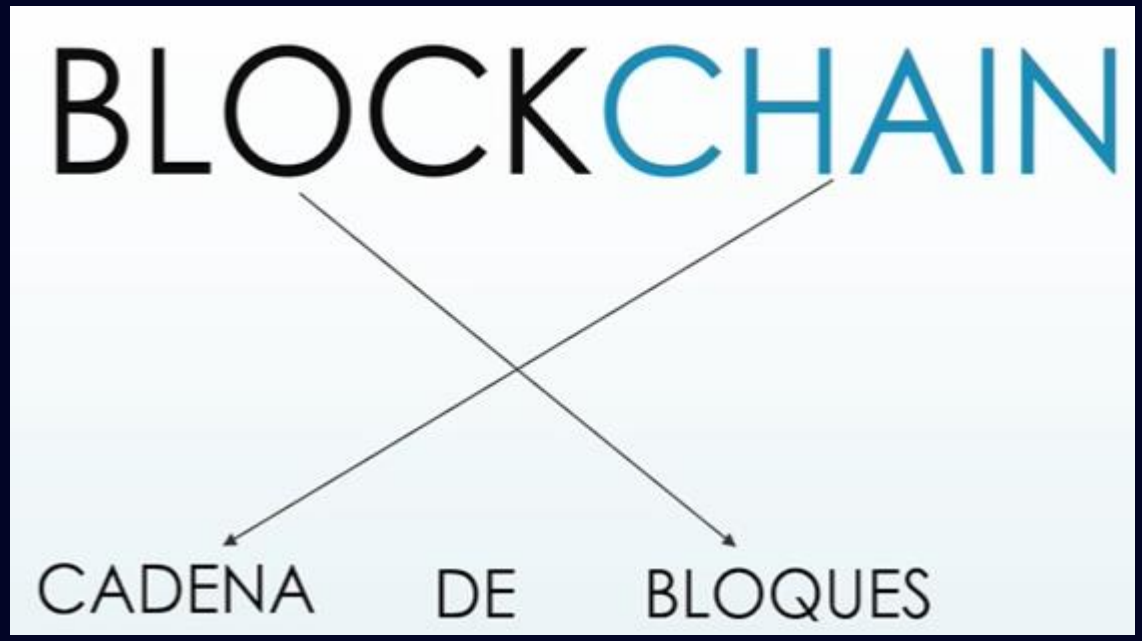
Recompensa 100 GranadaCoin

Bloque	Transacciones	Problema	Libro Mayor
1	----------	78 - ? – 12 = 40	Clave Pública A recibe 100
2	Clave Pública A envia 50 a Clave Pública B	45 + ? + 2 = 94	Clave Pública A envia 50 a Profesor B Clave Pública C recibe 100
3	Clave Pública A envia 10 a Clave Pública D Clave Pública C envia 40 a Clave Pública E	20 - ? + 2 = 12	Clave Pública A envia 10 a Clave Pública D Clave Pública C envia 40 a Clave Pública E Clave Pública A recibe 100

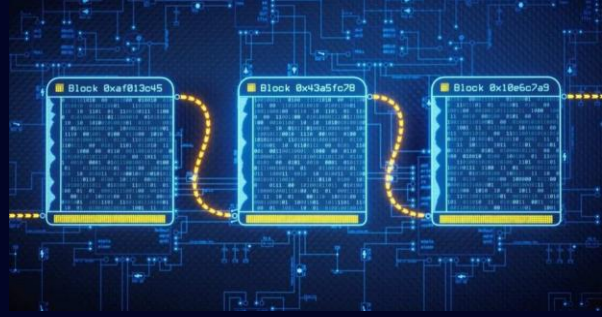


Blockchain

Blockchain



Blockchain



Generación de bloques

Cada bloque se va llenando con transacciones que los usuarios mandan a la red.

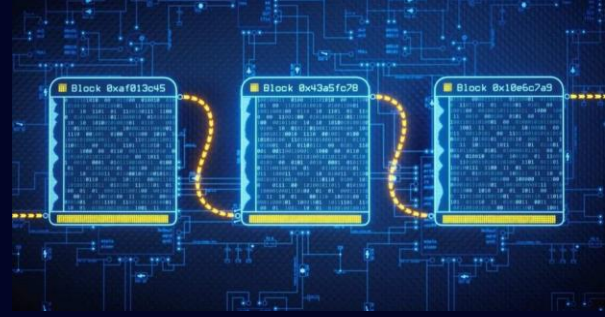
Un bloque tiene un tamaño determinado, el cual se determina en el White Paper de cada criptomoneda

Libro de registro

Con la blockchain o cadena de bloques tendremos un libro o registro de la actividad de esa red donde estarán presentes todas las transacciones ocurridas desde la creación de esa red.

Este libro es **INMUTABLE**, no podrá ni eliminarse ni modificarse.

Blockchain

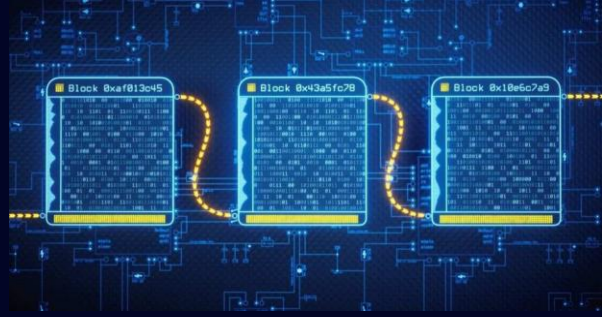


¿Cómo se producen las transacciones en una blockchain?

Las transacciones tienen que ser comprobadas o verificadas por la red. Es decir, si Pedro tiene que enviar criptomonedas a Pablo, la red tiene que comprobar que Pedro tiene en realidad esas criptomonedas.

Este proceso de comprobación no es siempre el mismo, y cambia según el tipo de red o blockchain

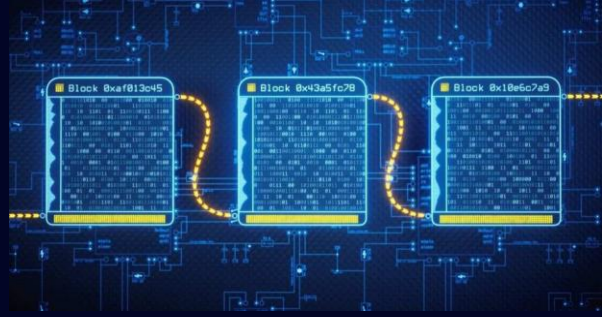
Blockchain



Transacción tradicional

Transacción en blockchain

Blockchain

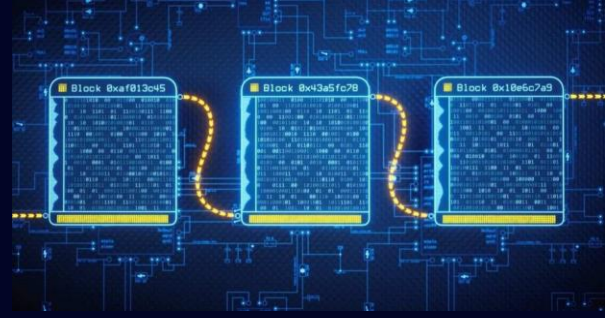


¿Qué es un nodo?

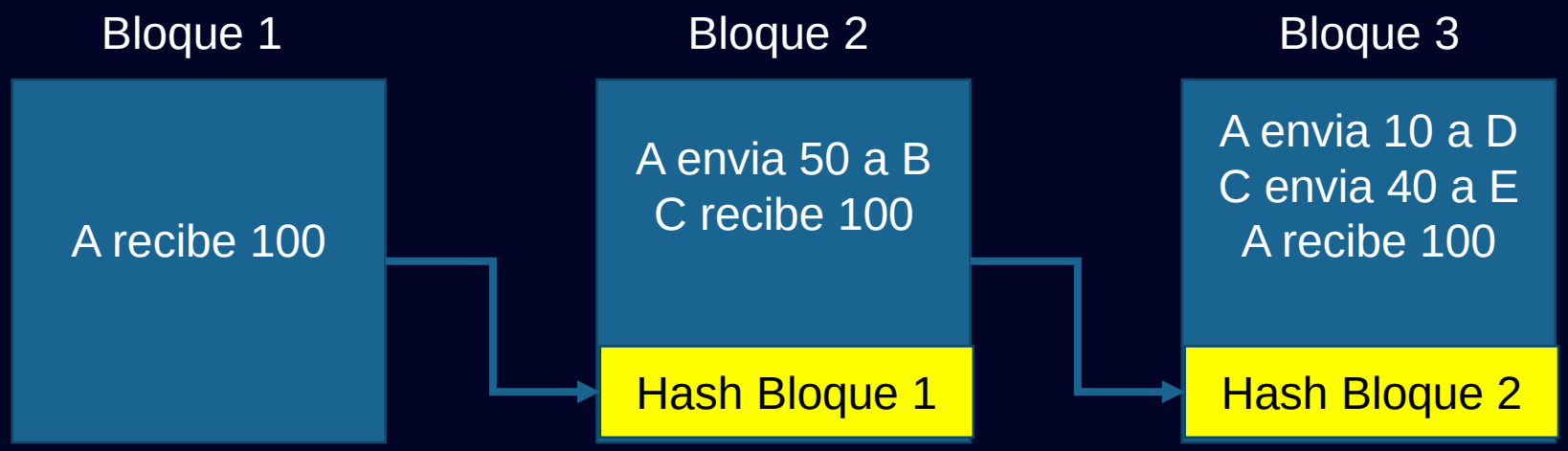
- Un nodo es un equipo conectado a la red blockchain, pero no todos los equipos conectados a la red son nodos.
- Siguen las reglas de la red y comparten información.
- Alojan y sincronizan una copia del libro de registro con todas las transacciones de la red, es decir, una copia de toda la blockchain.

La red no puede funcionar sin los nodos.

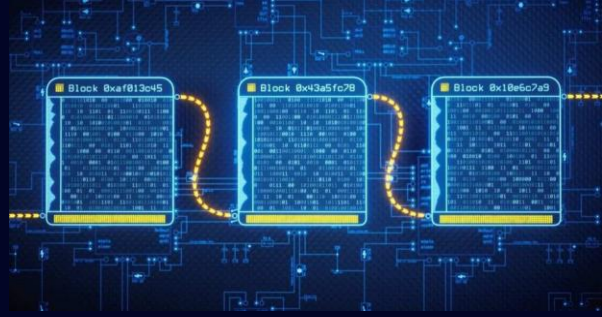
Blockchain



Cadena de bloques en blockchain GranadaCoin



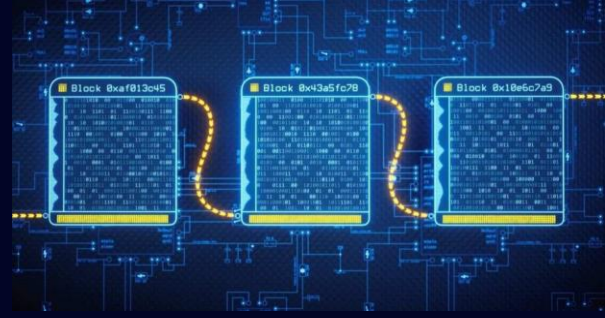
Blockchain



Protocolos de consenso

- Cuando un bloque se llena de transacciones, se cierra y se pasa por un proceso para añadirlo a la red de manera que quede “sellado” (inmutable e inalterable).
- Para que esto ocurra, los nodos se tienen que ponerse de acuerdo. Un nodo no puede escribir por si solo un bloque o añadirlo a la red.
- Los nodos tienen de alguna manera que entenderse y ponerse de acuerdo. Esas “reglas del juego” es a lo que nos referimos con protocolos de consenso.

Blockchain

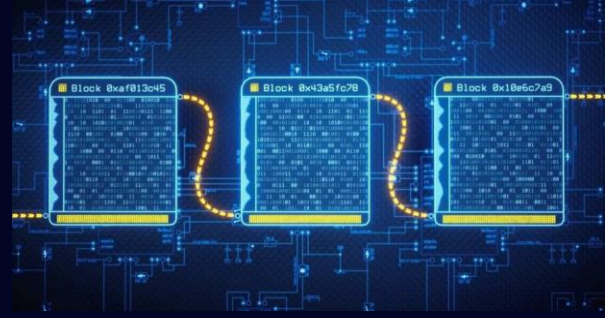


PoW (Proof of Work) – Prueba de Trabajo

- Quizás el protocolo más conocido (el que usa Bitcoin).
- Participan todos los nodos de la red de forma seudónima
- Los equipos compiten entre si para sellar un bloque
- Los equipos deben resolver un algoritmo complejo para lograr el objetivo
- Cuanto mayor poder de procesamiento tenga el equipo, más posibilidades de resolver el algoritmo y sellar el bloque
- Consume mucha energía debido al trabajo que el equipo debe hacer

La recompensa se la llevará el primer equipo que resuelva el algoritmo.

Blockchain



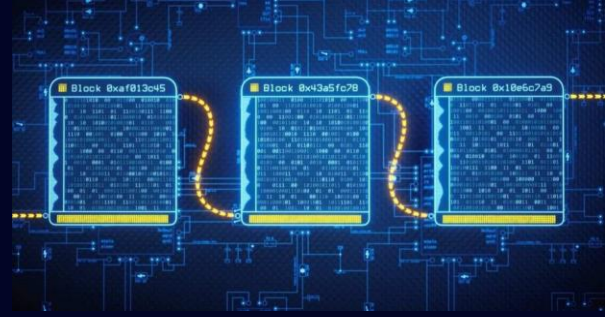
PoW (Proof of Work) – Prueba de Trabajo

Los usuarios envían transacciónes a la Red

Los nodos recolectan las transacciones y forman un bloque “resuelto”

La mitad + 1 de los nodos verifican el bloque. Se sella y todos los nodos lo añaden a su cadena

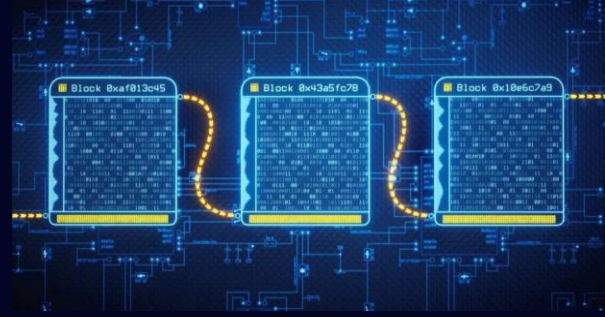
Blockchain



PoS (Proof of Stake) – Prueba de Participación

- Es el protocolo de mayor uso después del PoW
- En este proceso no importa si tu equipo tiene mayor poder de procesamiento o menos. No importa si el equipo es mas moderno o antiguo
- La probabilidad que tienen cada nodo para resultar elegido y poder sellar el bloque estará supeditado al número de criptomonedas de esa red que el nodo posea

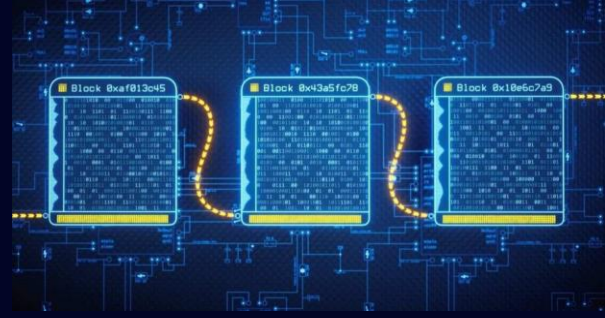
Blockchain



PoS (Proof of Stake) – ¿Qué es el Staking?

- Se conoce como Staking al proceso de dejar depositadas tus criptomonedas “trabajando” para hacer que funcione el PoS y con ella la red y así poder conseguir esa rentabilidad
- Este proceso solo existe en redes cuyo protocolo de consenso es PoS
- Existen otros procesos parecidos para conseguir rentabilidad, pero no son Staking (aunque se les llame así)

Blockchain



Ventajas o diferencias entre el PoS y el PoW

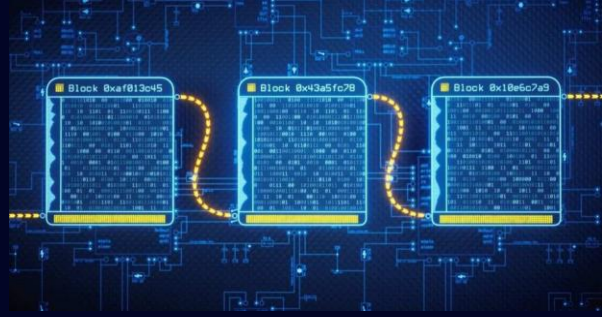
PoS

- Se consume muy poca energía
- Bajo coste inicial y retorno de inversión mas fácil
- Favorece la compra del activo pero no tienen un precio de producción

PoW

- Alto consumo de energía
- Alto coste inicial y riesgo por degradación / antiguedad
- Más presión de venta pero como tiene coste de producción añade valor al activo

Blockchain



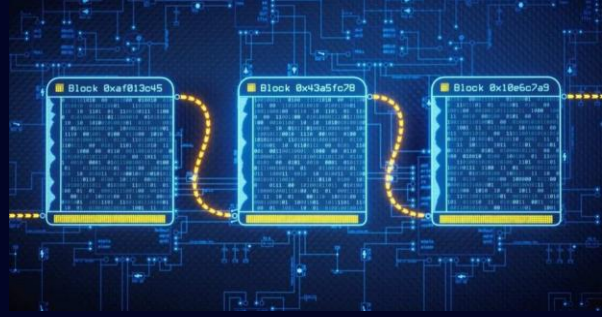
Otros protocolos

PoA (Proof of Authority) – Prueba de Autoridad

DPoS (Delegate Proof of Stake) – Prueba de participación delegada

Y muchos mas en pruebas o desarrollándose.

Blockchain



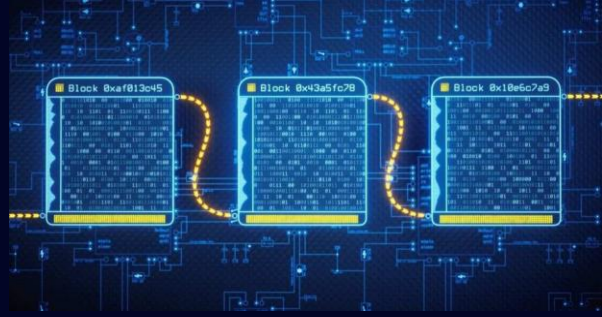
Minería

Como la red bitcoin funciona con un protocolo PoW, los equipos tendrán que tener una capacidad de proceso grande para ser rentables y esto con el tiempo ha ido creando una forma de negocio muy concreta buscando equipos con mejor proceso y a la vez formas más baratas de conseguir la energía necesaria.

Recursos
- Procesadores / CPUs
- Tarjetas gráficas
- Equipos específicos diseñados para ello

El elevado consumo de energía ha agudizado el ingenio de las personas o entidades que se dedican a la minería de bitcoin

Blockchain

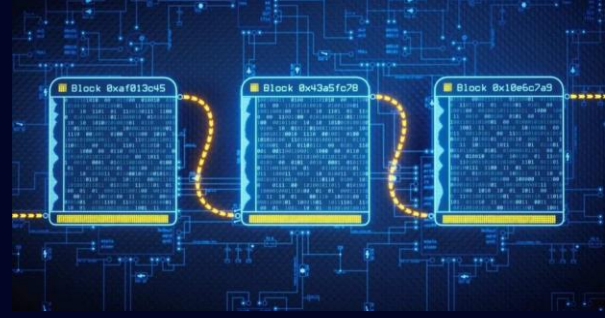


Halving

En la red de Bitcoin, y en algunas más, la recompensa que reciben los mineros se ve reducida a la mitad en unos eventos llamados Halvings. Esto es, después de cada Halving, el número de criptomonedas que se van generando es menor (la mitad).

Este proceso de reducción es automatizado y periódico y se utiliza principalmente para controlar la emisión de la criptomoneda.

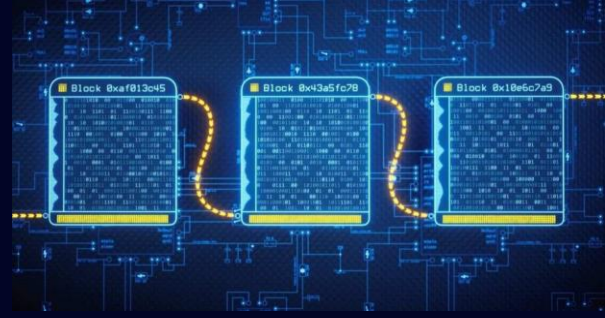
Blockchain



Halving - Bitcoin

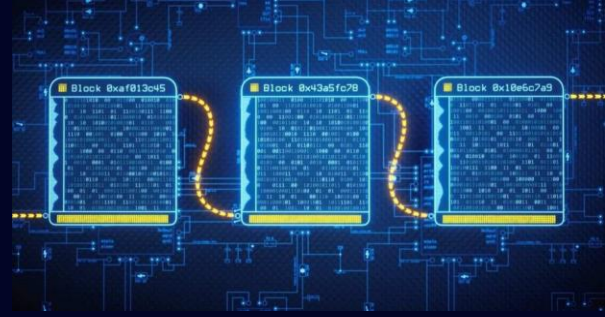
Fecha	Recompensa	BTCs emitidos
2008 (Inicio)	50 BTCs	0
2012	25 BTCs	10,5 millones
2016	12,5 BTCs	15,75 millones
2020	6,25 BTCs	18,37 millones
2024	3,125 BTCs	19,7 millones
----------	----------	----------
2140	0 BTCs	21 millones

Blockchain



Halving - ¿Afecta al precio?

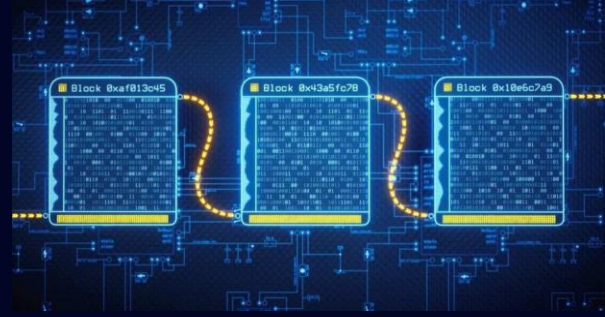
Blockchain



Halving - ¿Por qué es relevante?

- Sirve para controlar la emisión del activo
- Facilita el acceso a la moneda en las fases tempranas y genera una escasez futura
- Genera ciclos de mercado vinculados al valor de la moneda
- Produce un periodo de mejora en la eficiencia de equipos informáticos y eficiencia energética de la minería y con ello de la red

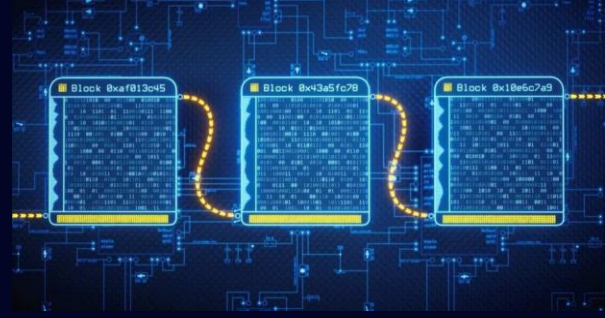
Blockchain



Halving - ¿Qué ocurrirá con los mineros tras el último Halving?

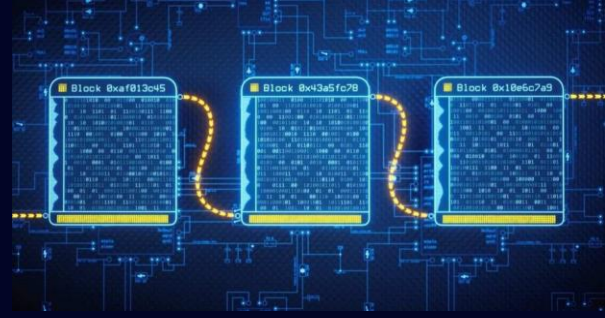
Llegado ese punto en el que ya no se emitan nuevas criptomonedas, cada vez que se valide y se selle un bloque, los mineros continuarán obteniendo recompensas en forma de comisiones de la red, es decir, las fees que los usuarios pagan por cada transacción.

Blockchain



Entre un 17 y un 23% de los bitcoins existentes están perdidos en el olvido, según un estudio

Blockchain



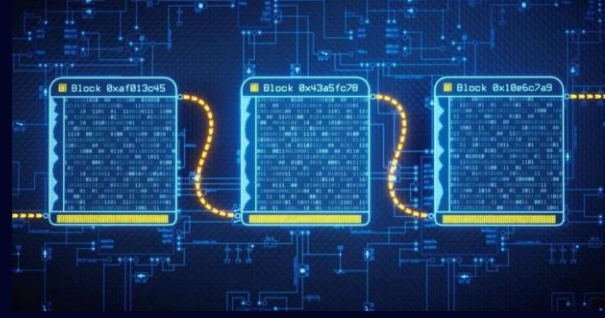
Tipos de blockchains

Públicas No permisionadas → son aquellas a las que cualquiera puede unirse en cualquier momento, como Bitcoin o Ethereum. No disponen de privacidad, y todos los usuarios son seudónimos. Como los participantes no están identificados, es difícil poder obligar a que las transacciones y las aplicaciones cumplan la normativa, y perseguir a aquellos que no lo hagan. Existen costes por transacción.

Publicas, permisionadas → son aquellas en las que un consorcio o agrupación inicia una red y permite que cualquiera se una siempre que cumpla una serie de requisitos, como estar autenticados y cumplir con la regulación. Son abiertas, transparentes, descentralizadas y, por lo general, sin costes por transacción.

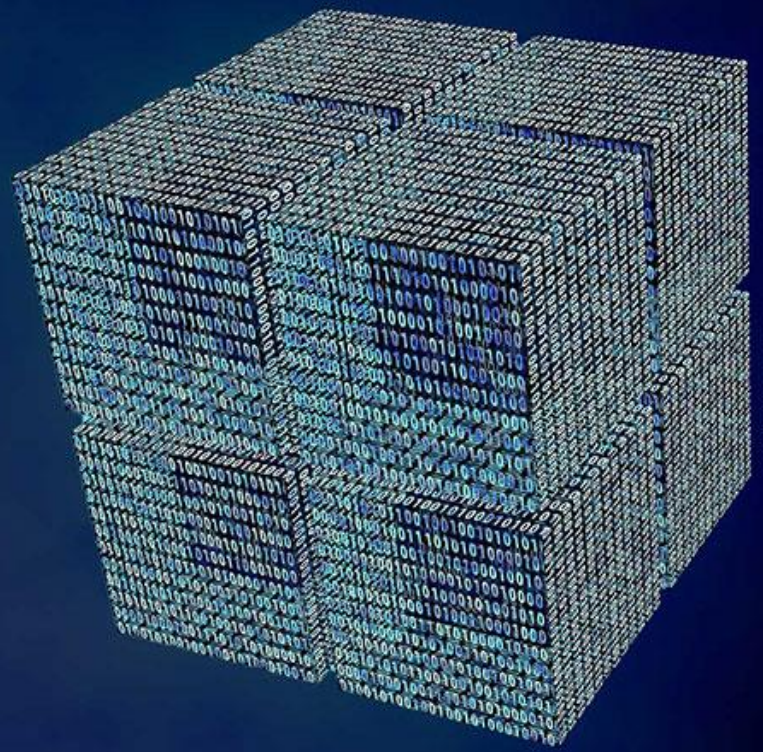
Privadas, permisionadas → son aquellas en las que una entidad privada ejecuta y mantiene todos los nodos. Suelen ser mantenidas por un proveedor de servicios de blockchain. Por lo general, no tienen costes de transacción y permiten privacidad. No son descentralizadas ni transparentes, la escalabilidad es muy limitada y generalmente están diseñadas para un solo uso o aplicación

Blockchain



"La interoperabilidad es el reto más grande": así es la carrera en Europa para lanzar las futuras 'carteras digitales' a ciudadanos y empresas

Alberto R. Aguiar 8 ago. 2022 7:30h.



Ethereum, Altcoins y Tokens

Ethereum, Altcoins y Tokens

Bitcoin no es perfecto. Su codificación no permite que su red, su plataforma, su trabajo en sí se utilice para otros proyectos o ideas más allá de para lo que fue creado

Ejemplo
Imaginad que tenemos un BTC y queremos enviarlo a un amigo, pero solo en el caso de que se cumplan ciertas condiciones, por ejemplo, en su cumpleaños.
Bitcoin no puede hacer eso, necesita de otras plataformas externas

Ethereum

Ethereum nace para cambiar eso.

¿Quién crea Ethereum? → Vitalik Buterin, que por aquel entonces era un niño prodigio de la informática, la programación y la codificación, fue el creador del proyecto en Julio 2015.
También intervinieron otros programadores que ahora son conocidos por toda la comunidad.

Ethereum

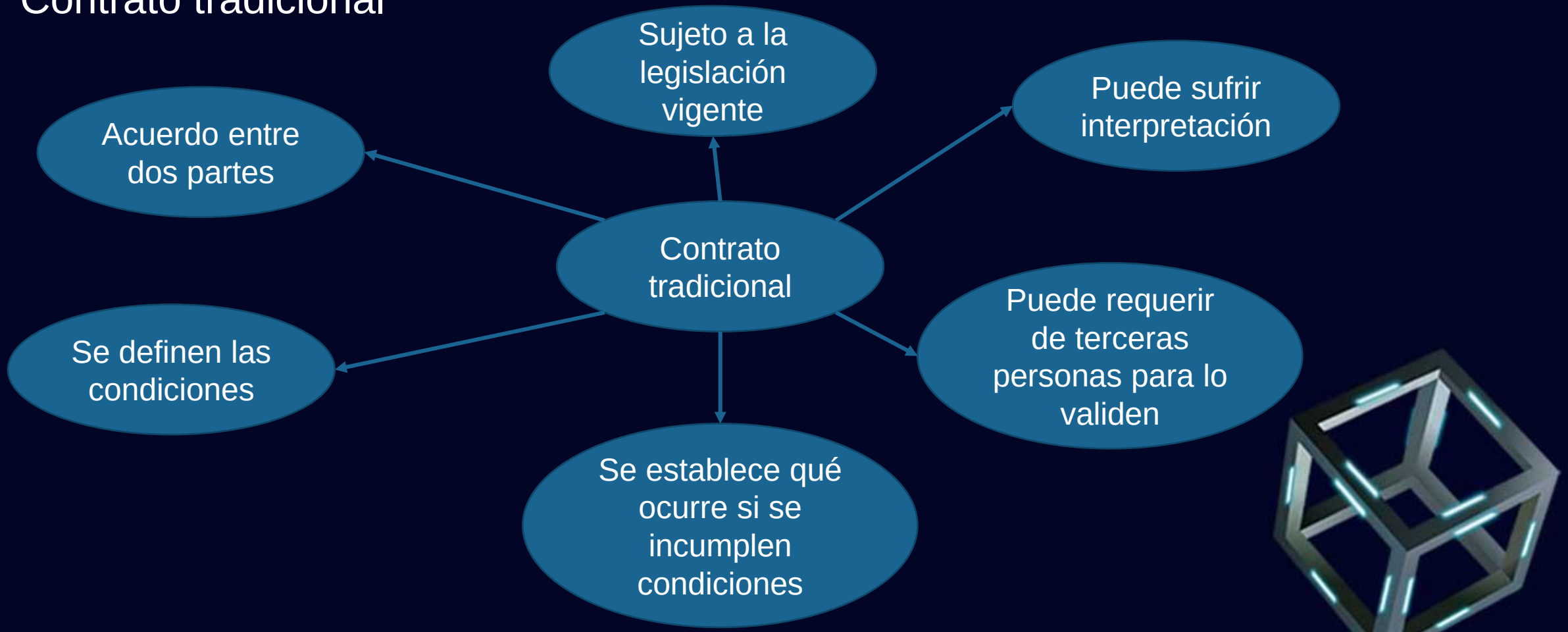
¿Qué cambia Ethereum?

La red de Ethereum no es muy diferente a la de Bitcoin, pero su lenguaje de programación le permite a los desarrolladores o creadores de aplicaciones crear software a través del cual gestionar transacciones o automatizar ciertos procesos dentro de esa red.

SMART CONTRACT → CONTRATO INTELIGENTE

Ethereum

Contrato tradicional



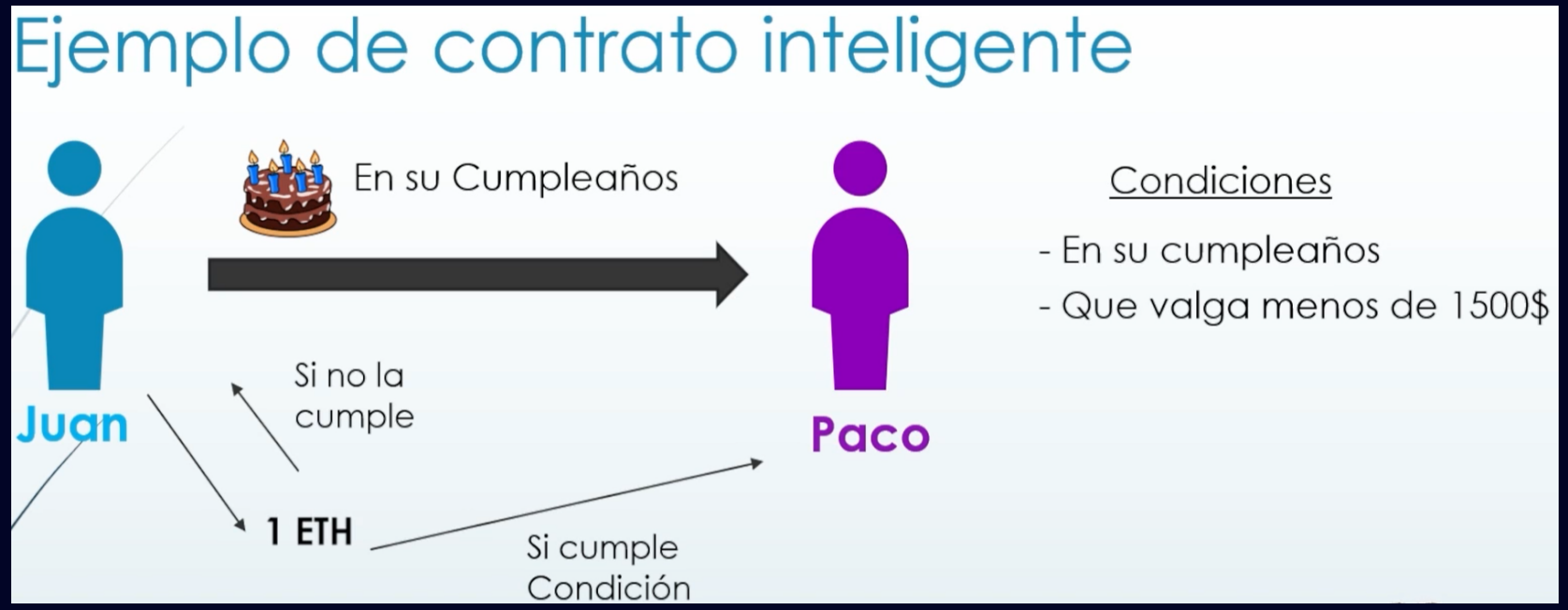
Ethereum

Contrato inteligente

- Un programa, aplicación o código
- Se ejecuta de manera automática cuando se cumplen las condiciones establecidas en el código
- Visible por todos, pero no modificable
- El contrato es público (está en la blockchain)

Ethereum

Contrato inteligente - Ejemplo



Todo eso estaría escrito y codificado en el “Smart Contract”

Ethereum

¿Cómo se firma un contrato inteligente?

La interacción con contratos inteligentes se realiza por lo general mediante el uso de billeteras

Algunos protocolos que usan contratos inteligentes:

- SWAP – Para intercambiar unas criptomonedas / tokens por otros
- LEND – Podemos prestar nuestros tokens a cambio de una rentabilidad
- Token – Creación de Tokens
- NFT – Tokens especiales, únicos y diferentes entre sí.
- Otros…

Ethereum

Ethereum no es solo una blockchain con una criptomoneda. Es toda una infraestructura pública en la que se pueden construir proyectos con sus propias criptomonedas

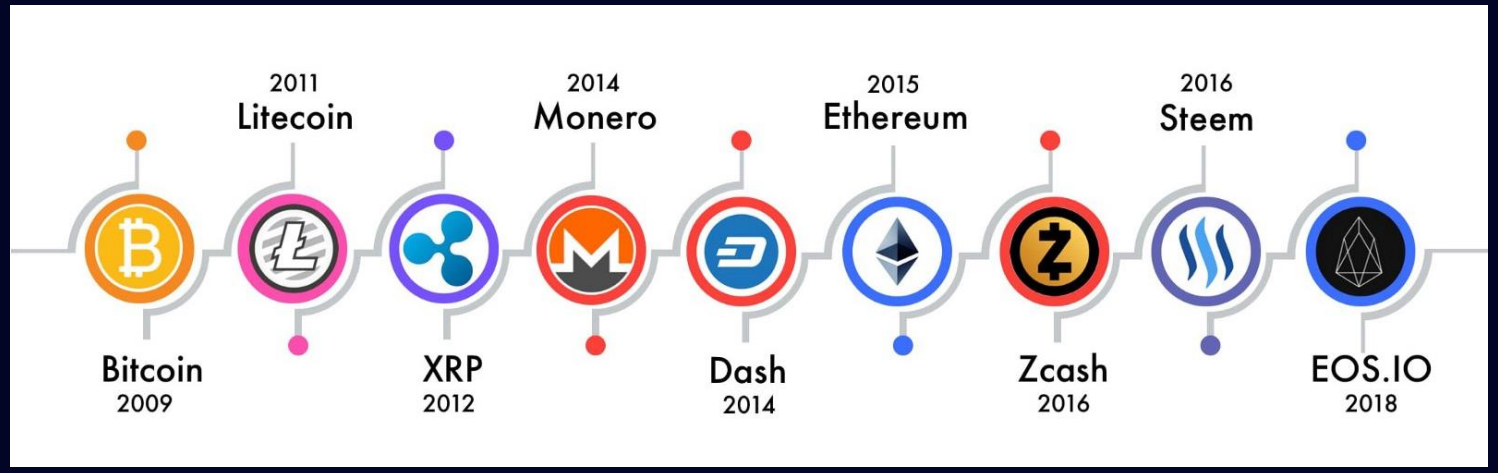
En lugar de codificar toda una nueva red completa, puedo usar la red de Ethereum y que mis monedas puedan ir circulando y gestionándose dentro de la red, con lo que eso conlleva en ahorro de tiempo y de dinero

El nacimiento de Ethereum abrió las puertas a un mundo nunca antes visto y fue realmente a partir de ese punto donde empezó la explosión de las criptomonedas y todo su ecosistema

Altcoins

¿Qué es una Altcoin?

Una Altcoin es toda aquella criptomoneda que no es Bitcoin.



Altcoins

Historical Snapshot - December 01, 2013

USD

#	Name	Symbol	Market Cap	Price	Available Supply
1	Bitcoin	BTC	$ 13,063,515,820	$ 1,083	12,060,836
2	Litecoin	LTC	$ 934,938,972	$ 39.77	23,505,833
3	Ripple	XRP	$ 367,702,839	$ 0.047034	7,817,889,792 *
4	Peercoin	PPC	$ 149,686,927	$ 7.58	19,755,711
5	Namecoin	NMC	$ 73,869,346	$ 9.94	7,435,150
6	Megacoin	MEC	$ 44,799,026	$ 2.13	21,081,586
7	Feathercoin	FTC	$ 29,697,306	$ 1.20	24,696,360
8	WorldCoin	WDC	$ 23,950,574	$ 0.722258	33,160,694
9	Primecoin	XPM	$ 22,417,311	$ 6.76	3,314,162
10	Freicoin	FRC	$ 16,367,128	$ 0.484410	33,787,745
11	Novacoin	NVC	$ 12,392,739	$ 24.63	503,110

February 09, 2020

1	Bitcoin BTC	$10,078.42	$183.52 B	$5.69 B
2	Ethereum ETH	$225.58	$24.73 B	$1.70 B
3	XRP XRP	$0.2798	$12.12 B	$669.38 M
4	Bitcoin Cash BCH	$444.08	$8.11 B	$849.87 M
5	Bitcoin SV BSV	$339.85	$6.21 B	$1.05 B
6	EOS EOS	$4.9233	$5.02 B	$359.86 M
7	Litecoin LTC	$76.30	$4.91 B	$891.03 M
8	Tether USDT	$0.9996	$4.64 B	$6.77 B
9	Binance Coin BNB	$23.85	$3.71 B	$118.97 M
10	Tezos XTZ	$2.6061	$2.11 B	$16.65 M

Altcoins

Septiembre 2022 - https://coinmarketcap.com/

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$21,566.12	0.15%	1.12%	9.64%	$413,310,033,718	$34,464,621,679 1,596,649 BTC	19,147,487 BTC	
2	Ethereum ETH	$1,759.07	0.05%	2.56%	13.62%	$215,302,902,485	$12,328,178,201 7,004,249 ETH	122,324,250 ETH	
3	Tether USDT	$1.00	0.00%	0.01%	0.03%	$67,671,319,499	$48,794,628,738 48,780,845,158 USDT	67,652,203,603 USDT	
4	USD Coin USDC	$0.9999	0.00%	0.01%	0.02%	$51,675,986,045	$5,529,907,432 5,530,637,809 USDC	51,682,811,280 USDC	
5	BNB BNB	$294.97	0.53%	0.51%	6.72%	$47,589,917,356	$770,782,037 2,613,072 BNB	161,337,261 BNB	
6	Binance USD BUSD	$1.00	0.00%	0.00%	0.02%	$19,999,960,766	$8,714,377,903 8,715,851,350 BUSD	20,003,342,405 BUSD	
7	XRP XRP	$0.3554	0.10%	0.30%	7.81%	$17,722,042,935	$643,964,579 1,810,524,512 XRP	49,826,021,773 XRP	
8	Cardano ADA	$0.5142	1.51%	0.70%	4.28%	$17,575,020,109	$749,815,050 1,458,331,824 ADA	34,182,044,153 ADA	
9	Solana SOL	$34.59	0.60%	0.01%	10.95%	$12,219,755,520	$670,300,892 19,379,000 SOL	353,284,096 SOL	
10	Polkadot DOT	$7.70	0.09%	0.11%	7.07%	$8,603,488,955	$262,239,759 34,006,533 DOT	1,115,676,875 DOT	

Altcoins

June 2021

Tokens

Como comentábamos anteriormente, Ethereum no es solo una blockchain con una criptomoneda

Redes como Ethereum permiten el desarrollo de aplicaciones o funcionalidades automatizadas, entre ellas, la creación de activos (tokens) que funcionen en la misma red.

Los tokens no son criptomonedas

Tokens

Token → Activo digital criptográfico sin red propia

Se mueven dentro de la red de la misma manera que si fueran la criptomoneda nativa de esa red en la que operan, y se sirven de sus funciones

Tienen diferentes características a la criptomoneda nativa

Supply, tasa de emisión, etc

Pero si la red principal se cae o no funciona, tampoco se podrá operar con los tokens existentes en esa red

Tokens

Algunos tipos de Tokens

Utility Token
Tienen un uso concreto (como comprar artículos, pagar pro servicios, etc)

Community Token
Comunidad o colectivo concreto (videojuego, miembros de un club, etc)

Asset Token
Representan objetos físicos u otros entes (oro, propiedades inmobiliarias, materias primas, ganado, etc..)

Se puede crear un token para cualquier cosa y los contratos inteligentes les hace especialmente útiles

Tokens

Algunos ejemplos de Tokens

USDT → Presente en la red de Ethereum y representa el valor de 1 dólar.

CAKE → Presente en la red de Binance, es el token utilizado en el proyecto PancakeSwap

Existen miles… y sigue creciendo

Tokens

Stablecoins

- Son tokens que operan en la red en que son creados
- Sirven como reserva de valor o liquidez
- Mantienen un valor estable asemejado a una moneda FIAT (Dólar, por ejemplo)

Tokens

Stablecoins mas conocidas

BUSD → Respaldado por Binance
USDC (USD Coin) → Respaldo por Coinbase
USDT → De la empresa Tether

USDT Tether La más utilizada

Esta mantiene un valor en torno a 1 dólar estadounidense. 1 USDT = 1 USD

Tienen guardados a modo de respaldo un dólar estadounidense por cada USDT que hay en el mercado.
"Según la empresa (TETHER)"

Tokens

Tokens envueltos (wrapped tokens)

- Tokens que representan el valor de otro token o criptomoneda
- El activo principal funciona en otra red
- No son el activo principal pero su valor es 1 a 1 con su homologo
- En la práctica, unen diferentes redes o blockchains

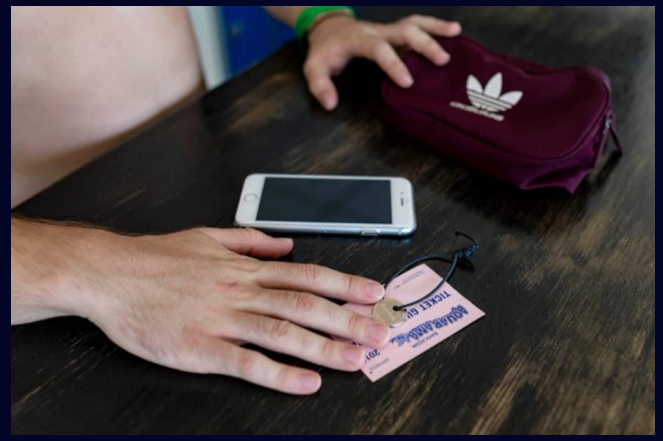
Un ejemplo → WBTC (Wrapped BTC) es un token envuelto de Bitcoin que se mueve de Ethereum representando a BTC.

Un BTC no es lo mismo que un WBTC pero valen lo mismo

Tokens

Tokens envueltos – ¿Cómo funcionan?

Pensemos en lo que ocurre con un ticket ropero



Tokens

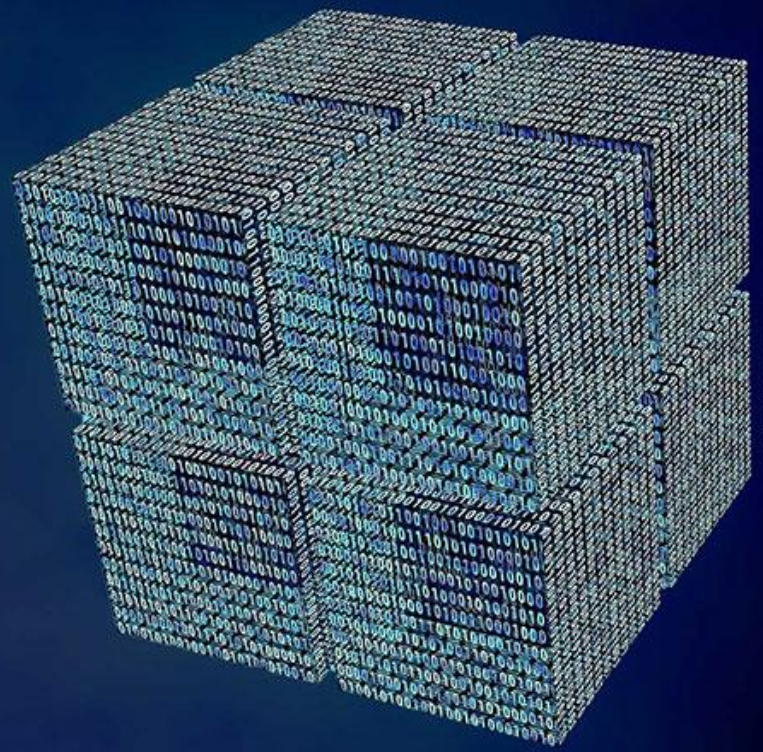
Tokens envueltos – ¿Cómo funcionan?

Hay un custodio, que se queda el BTC y te da a cambio el WBTC

- Empresa, Exchange, etc.
- Guardan la misma cantidad de la criptomoneda nativa que del token que emiten
- Puede ser el mismos smartcontract

Ejemplos

- WBTC: Bitcoin dentro de la red de Ethereum
- BTCB: Bitcoin dentro de la red de Binance
- WBNB: Binance coin dentro de la red de Ethereum



Transacciones y Billeteras

Billeteras

¿Dónde se guardan las criptomonedas?

Libro de registro de transacciones
Es el elemento base de todo proyecto blockchain. Contiene una copia de todas las transacciones realizadas por esa red o blockchain desde su creación. Cada nodo almacena una copia.

Las criptomonedas NO SE GUARDAN en ningún sitio. Ni en un ordenador, ni en una billetera, ni si quiera en la blockchain. Las criptomonedas como tal, no existen…son simplemente una anotación en ese Libro de registro.

¿Entonces qué se envía / reciben en cada transacción?

- No se envía / recibe nada.
- Solo se añade un asiento en el Libro de Registro cambiando la titularidad.

Billeteras

REDES

Cada criptomoneda opera en una blockchain determinada. Por ejemplo no puedo mandar Bitcoin en la red Ethereum.

CUANDO SE ENVIA UNA CRIPTOMONEDA A OTRO USUARIO, ESTE ENVÍO O TRANSACCIÓN SE TIENE QUE HACER USANDO SU PROPIA RED.

Cuando operamos en un Exchange, la plataforma nos suele (debe) preguntar por qué plataforma queremos hacer el envío. Esto hay que tenerlo muy claro, y es una gran responsabilidad por el riesgo que supone.

Billeteras

PROBLEMAS COMUNES

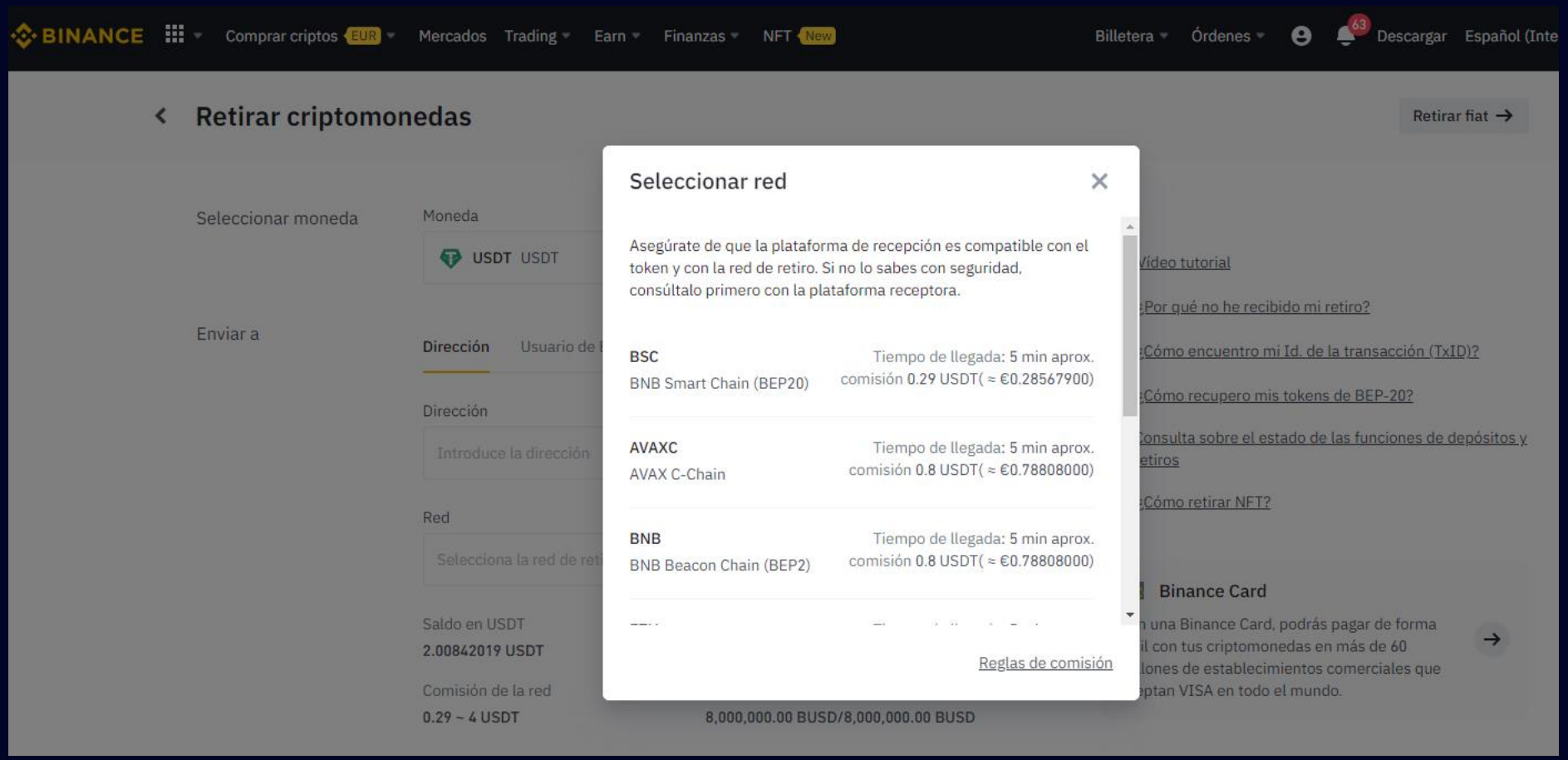
Error al seleccionar la red de envío

Si yo envío Ethereum usando la red de otra criptomoneda, esta transacción puede que nunca llegue a su destinatario y los fondos se pueden perder de forma irremediable.

Error en el destino

Si al hacer una transacción elegimos bien la red, pero la dirección donde la enviaos no pertenece a esa red, también se pueden perder los fondos.

Billeteras


BINANCE
Comprar criptos EUR
Mercados
Trading
Earn
Finanzas
NFT New
Billetera
Órdenes
63
Descargar
Español (Inte
Retirar criptomonedas
Retirar fiat
Seleccionar moneda
Moneda
USDT USDT
Enviar a
Dirección
Usuario de
Dirección
Introduce la dirección
Red
Selecciona la red de reti
Saldo en USDT
2.00842019 USDT
Comisión de la red
0.29 ~ 4 USDT
8,000,000.00 BUSD/8,000,000.00 BUSD
Seleccionar red
Asegúrate de que la plataforma de recepción es compatible con el token y con la red de retiro. Si no lo sabes con seguridad, consúltalo primero con la plataforma receptora.
BSC
BNB Smart Chain (BEP20)
Tiempo de llegada: 5 min aprox.
comisión 0.29 USDT(≈ €0.28567900)
AVAXC
AVAX C-Chain
Tiempo de llegada: 5 min aprox.
comisión 0.8 USDT(≈ €0.78808000)
BNB
BNB Beacon Chain (BEP2)
Tiempo de llegada: 5 min aprox.
comisión 0.8 USDT(≈ €0.78808000)
Reglas de comisión
Vídeo tutorial
¿Por qué no he recibido mi retiro?
¿Cómo encuentro mi Id. de la transacción (TxID)?
¿Cómo recupero mis tokens de BEP-20?
Consulta sobre el estado de las funciones de depósitos y retiros
¿Cómo retirar NFT?
Binance Card
una Binance Card, podrás pagar de forma
il con tus criptomonedas en más de 60
lones de establecimientos comerciales que
ptan VISA en todo el mundo.

Billeteras

Billeteras y direcciones

- Ya sabemos que las criptomonedas no se guardan en ningún sitio, pero si necesitamos de algo que nos de el derecho a la gestión de esos activos (un apunte en el libro de registro)
- La billetera es la que nos permite ese acceso y gestión, además de ser la que indica la titularidad de esos activos.
- Así que de una manera “errónea” pero acertada, de forma generalizada se define como billetera (wallet) como el sitio donde podemos guardar nuestras criptomonedas.

Billeteras

Tipos de billeteras

- Billeteras calientes (hot wallets)
- Billeteras frías (cold wallets).
- Billeteras gestionadas por Exchanges.

Billeteras

Hot Wallets

- Se llaman billeteras calientes por el riesgo mayor que tienen
- Están de manera permanente conectadas a internet (desde el ordenador, aplicación móvil, etc) y por tanto son mas vulnerables a hackeos o algún software espía que pueda acceder a las contraseñas, números de seguridad, etc.
- Son más rápidas, intuitivas y fáciles de usar debido a que su conexión continua a la red le da una utilidad mayor dándonos accesos a servicios web3.

Algunos ejemplos

- Metamask (PCs)
- Trustwallet (móvil)
- Phatom (PCs)
- …..

Billeteras

Cold Wallets

- Se llaman billeteras frías por ser de menor riesgo. Son las más seguras.
- No se conectan a internet en ningún momento, solamente en el instante de hacer el envío a otras personas o usuarios.
- El hecho de no conectarse a internet y no compartir información sensible con ningún equipo informático las hace mas seguras a hackeos o softwares espía.

Algunos ejemplos

- Ledger
- Trezor
- Safepal
- …..

Billeteras

Gestionadas por Exchanges

- Funcionan como los bancos tradicionales.
- Son plataformas donde puedes gestionar tus criptomonedas de una manera indirecta, ya que son ellos los que custodian los fondos. La billetera de envío será la del propio Exchange, que una vez recibida la transacción, te actualizará el saldo en tu cuenta de usuario.
- En este caso, tu NO tienes la propiedad directa de tus criptomonedas.
- A día de hoy, no son el lugar mas recomendable ara tener tus criptomonedas mucho tiempo.

Billeteras

Direcciones

- Para poder hacer un envío, necesitamos saber a qué dirección hacerlo.
- Las direcciones son generadas por proceso de criptografía (codificado) y pueden compartirse sin riesgo alguno ya que ese código no da acceso a nuestros activos, simplemente permite a un usuario enviarnos criptomonedas.
- Cada red tiene sus procesos diferentes y las direcciones aunque similares, suelen tener aspectos que las diferencias algunas de otras.
- Una billetera, puede tener múltiples direcciones.

Billeteras

Direcciones - Ejemplos

Dirección de Bitcoin: bc1aykmfme23lsdwmerws4fck6

Dirección de Ethereum: 0xA2sdfwerr495sdf1we6werwf1cxv

Dirección de Tron: TBbym345ldfsdfsaso565msdwovtsssdlej

Direcciones – Utilidades con QR

Billeteras

Dominios ETH

Billeteras

Frase Semilla

- Consiste en una frase de 12 ó 24 palabras.
- Es la única vía para recuperar el control de tu billetera:
  - En billeteras calientes, si por ejemplo, pierdes el dispositivo (móvil, PC, Tablet, etc)
  - En billeteras frías, si pierdes el ledger, trezor, etc.
- Permite poder gestionar tu billetera desde distintos dispositivos (por ejemplo, cuando adquirimos uno nuevo).

¿Dónde guardarías tu frase semilla?

Transacciones

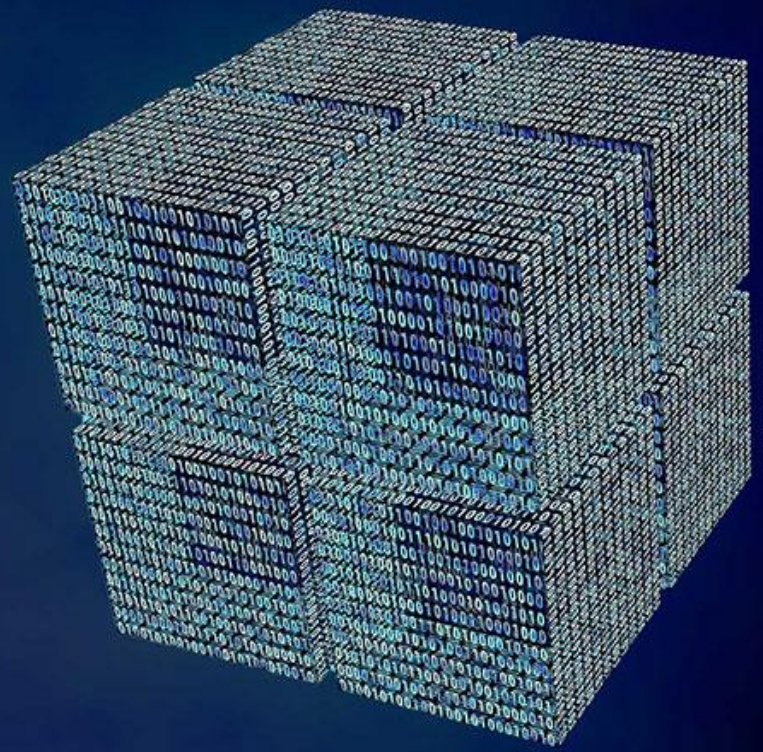
¿Qué necesito para hacer una transacción?

- Una billetera
- Saldo en alguna de las direcciones que tenga en la billetera.
- Dispositivo desde el que operar mi billetera (móvil ordenador, Tablet…)
- Una dirección de envío a donde quiera enviar.

Transacciones

Comisiones

- En las transacciones de criptomonedas, existen comisiones y pagos que se tienen que realizar por parte de quien envía las criptomonedas.
- Estas comisiones no son iguales en todas las redes y hay algunas mas económicas que otras.
- La diferencia puede ser tan grande que muchos usuarios pueden llegar a vender sus criptomonedas y cambiarlas por otras para usar así otra red a la hora de enviar sus activos.
- Los protocolos de consenso, impactan en la velocidad y también en las comisiones



Exchanges

Exchanges

¿Qué es un Exchange?

- Un Exchange es una casa de intercambio
- Son plataformas que ponen en contacto de una manera anónima a usuarios que quieren vender y a usuarios que quieren comprar
- Son creadores del Mercado
- También gestionan y custodian tus activos
- Es un concepto muy similar al del banco
- Los Exchanges usan tus activos (así como los bancos también lo hacen)

Exchanges

Cuentas de usuario

- Para operar en un Exchange, es obligatorio crear una cuenta de usuario
- Dependiendo del Exchange, para una cuenta básica, los datos que la plataforma pide son muy básicos (usuario / contraseña). Estas cuentas permiten operar hasta un máximo de capital
- Para acceder a servicios donde se vayan a superar esos máximos, todos los Exchanges obligan a pasar un proceso llamado KYC (Know Your Customer)
- En un proceso KYC, una persona se identifica mediante una serie de documentos
  - DNI, Pasaporte, Dirección, etc

Exchanges

Cómo puedo hacer un depósito en un Exchange para empezar a operar con criptomonedas?

- Tarjeta bancaria
- Transferencia bancaria
- Transferencia cripto

Cada Exchange va a elegir las criptomonedas con las que opera

Exchanges

Cotizaciones

- Cada activo tendrá una sección en el mercado
- El precio de un activo, se da en comparación con otros. Son los llamados PARES DE COTIZACION
- Ejemplos:
  - 1 BTC = 25.000€
  - 1 BTC = 27.000 $
  - 1 BTC = 12 ETH

Exchanges

Cotizaciones – Ejemplo, queremos comprar BTC y tenemos:

Terminaremos con un único activo: BTC

Exchanges

¿Quién fija el precio de una criptomoneda?

- El precio lo fijan los inversores
- Diferentes precios para cada cotización
- Diferentes precios en cada Exchange
- El precio fluctúa con el tiempo

Exchanges

Algunos Exchanges mas conocidos

coinbase

BINANCE

KUCOIN

kraken

bit 2 me

crypto.com

Exchanges

finanzas.com

IBEX 35 | Cotizaciones | Análisis técnico | Criptomonedas | Mercados | Jubilación | Finanzas personales | Fondos

Divisas

El Banco de España registra nuevas plataformas de criptomonedas pero sin vigilarlas

El Banco de España incluye en su registro a Binance, la mayor plataforma de criptomonedas del mundo, pero advierte de que no supervisará su actividad

FINANZAS.COM 8 JUL 2022 / 17:35

Coincidiendo con el cese de las operaciones de la empresa española de criptomonedas 2gether, que ha dejado atrapados en un corralito a 100.000 inversores, el Banco de España ha incluido en su registro de proveedores de servicios de monedas virtuales a **Moon Tech Spain**, la filial española de **Binance**, la mayor plataforma de criptomonedas del mundo.

Binance, que cuenta con unos 120 millones de usuarios en todo el mundo, está ganando impulso en Europa después de que Francia e Italia también la incluyeran en sus registros nacionales en los últimos meses, mientras la Unión Europea prepara una regulación del sector.

Exchanges

Exchanges descentralizados

- Tipo de Exchange donde no se necesita a otra persona que quiere vender para que tu puedas comprar
- No suele tener una empresa que sea dueña de esa liquidez. La liquidez la aportan los usuarios directamente
- Funcionan de una manera mucho más anónima para los usuarios
- También se les conoce como DEX

Exchanges

Exchanges descentralizados – Características

- Sin KYC
- No depositas capital en dinero FIAT (euros, dólares, etc)
- Conectas directamente tus billeteras calientes o frías
- Siempre que haya liquidez, puedes comprar o vender
- Suelen tener funciones adicionales de rentabilidad
- Deberás conocer la red en la que operan para poder hacer transacciones en ellos

Exchanges

Algunos DEX mas conocidos

PancakeSwap

Funciona en la red BNB (Binance)

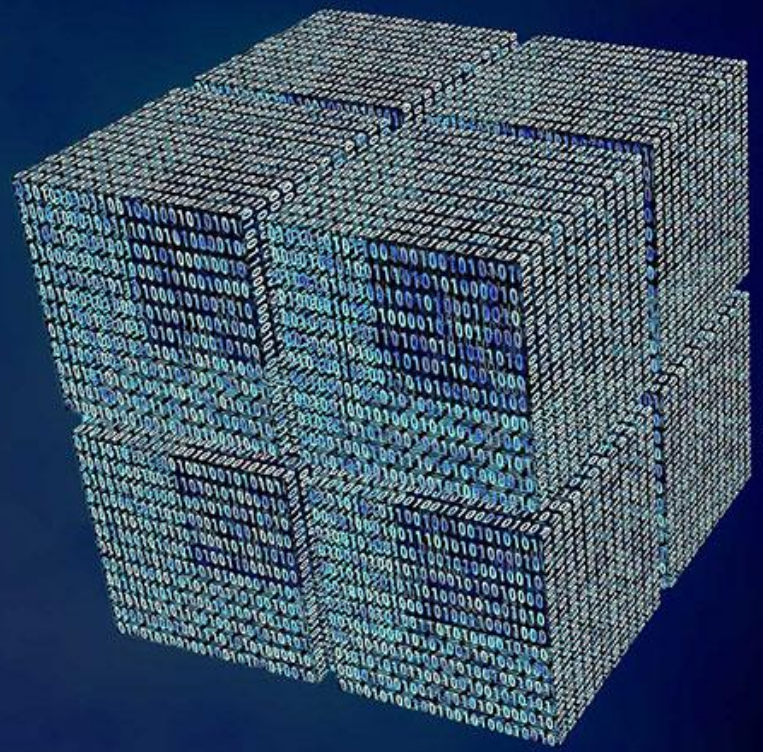
UNISWAP

Funciona en la Ethereum

Exchanges descentralizados

Tokens - Riesgos

- Cualquiera puede crear un Token
- Cualquiera puede ponerlo a disposición en un DEX
- Los DEX se nutren mayoritariamente por Tokens



Introducción a Defi

DEFI

DeFi significa “Decentralized Finance” o Finanzas Descentralizadas basadas en la no intervención de terceros y en el uso de smart contracts

Las primeras plataformas DEFI nacieron en la infraestructura Ethereum (Uniswap, fue una de ellas), pero pronto se extendieron a otras blockchains

Los proyectos DEFI en Ethereum siguen siendo con claridad los de mayor dominancia en términos de TVL (Total Value Locked) con un valor total de $34.31b

DEFI

Pools de Liquidez y SWAP

- En los DEX existe una liquidez depositada en forma de tokens (TVL)
- Esa liquidez la aporta el propio creador del token o por cualquier usuario o inversor del activo
- Se aporta en dos tokens o activos a la vez, para facilitar el mercado de un par de cotización concreto (ejemplo, BNB / BUSD)
- Esa liquidez se deposita de una forma ordenada y siguiendo unos determinados requisitos llamamos **Pools de Liquidez** (también se les conoce como piscinas de liquidez)
- Los pools de liquidez son los que hacen posible el intercambio de activos (SWAP) en los Exchanges descentralizados

DEFI

Pools de Liquidez – ¿Por qué aportar liquidez?

- Para ganar una rentabilidad.
- Al usar un DEX para cambiar un activo por otro, se pagan comisiones.
- Esas comisiones no son para el DEX, se reparten entre todos los que han aportado liquidez a ese par de intercambio

DEFI

Préstamos Descentralizados

- Al igual que en las finanzas tradicionales, en DeFi existen protocolos que facilitan los préstamos. La tasa de interés también está determinada por algoritmos y es calculada en función de la oferta y de la demanda de los activos

Algunas plataformas de Lending Descentralizadas:

- Aave
- Compound

DEFI

Blockchains mas importantes según su TVL y 3 proyectos mas grandes en cada una de ellas (Septiembre 2022)

- **Ethereum** (TVL - $34.31b) - **MakerDAO** ($7.89b), **LIDO** ($6.74b), **Uniswap** ($5.47b)
- **Tron** (TVL - $5.61b) - **JustLend** ($3.31b), **SUN**($1.19b), **JustStables** ($1.09b)
- **Binance Smart Chain** (TVL - $5.31b) - **PancakeSwap** ($2.99b), **Venus** ($693m), **Alpaca Finance** ($518m)
- **Solana** (TVL - $1.43b) - **Solend**($258m), **Marinade Finance**($241m), **Serum** ($196m)
- **Avalanche** (TVL - $1.78b) - **AAVE** ($764m), **Benqi**($308m), **Platypus Finance**($158m)
- **Polygon** (TVL - $1.76b) - **AAVE** ($360m), **MM Finance** ($347m), **QuickSwap** ($287m)
- **Arbitrum** (TVL - $975m) - **GMX**($296m), **Uniwap** ($101m), **Stargate** ($99m)
- **Optimism** (TVL - $911m) - **AAVE** ($434m), **Synthetix** ($170m), **Velodrome** ($68m)
- **Cronos** (TVL - $880m) - **VVS Finance** ($497), **Tectonic** ($228m), **Ferro** ($74)
- **Fantom** (TVL - $539) - **Spooky Swap**($122m), **Curve** ($60m), **Beefy** ($59m)

DEFI

DAO – Organización Autónoma Descentralizada

- Grupo, conjunto u organización de usuarios o entidades
- Se unen para un propósito en común
- Siguen unas reglas preestablecidas codificadas dentro de un programa, protocolo o contrato

DEFI

DAO – Caracteristicas

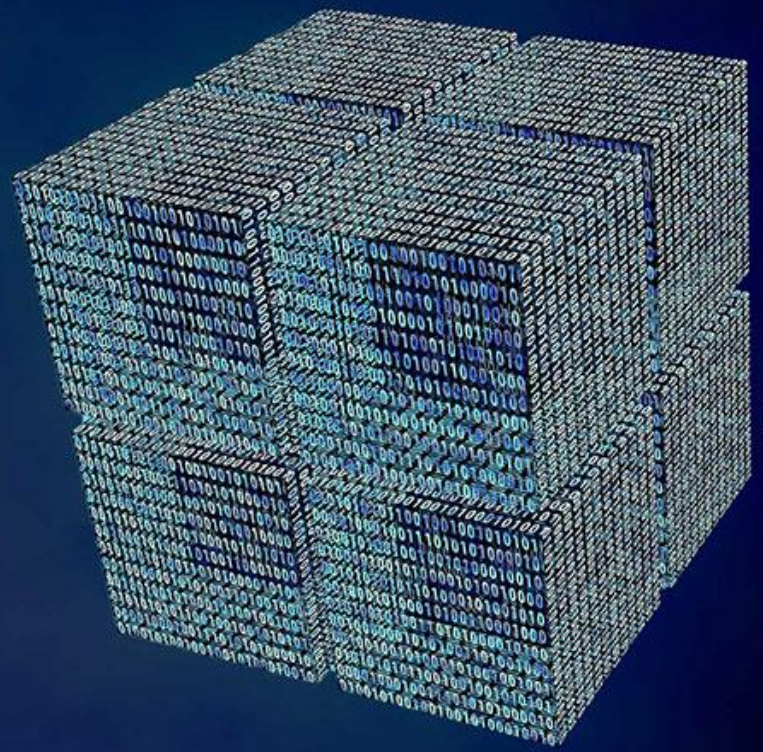
- **Autónomas**: No necesitan de incidencia externa
- **Autogestionadas**: su funcionamiento es automático
- **Transparentes**: Toda la información, actuaciones y progresos son visibles para todo el mundo
- **Capacidad de cambio**: cada miembro es libre de hacer propuestas que deberán ser votadas por el resto para decir si se aprueban o no

DEFI

DAO – Ejemplo

- Autoservicio
- Repone automáticamente esos productos sin necesidad de un gerente o encargado
- Los usuarios pueden proponer productos para que se vendan.
- La comunidad vota y si se acepta, la máquina hace el pedido

Todo se hace de manera automática



NFTs y Metaverso

NFT

Token No Fungibles (Non-Fungible Token)

- Los NFT son activos digitales únicos. No hay dos NFT que sean iguales
- Su unicidad viene confirmada en un certificado digital de autenticidad
- Los NFT suelen estar adjuntos a algunas obras o ilustraciones digitales
- Su precio es realmente el que la gente le quiera dar
- Toda la historia de un NFT está registrada en la blockchain donde opera

¿Por qué la gente compra NFTs?

NFT

Token No Fungibles - Usos

- Los usos posibles de los NFT son prácticamente infinitos
- En la actualidad, son muy usados en videojuegos y como coleccionables
- Algunos otros ejemplos:
  - Podrán dar acceso a servicios o ciertos privilegios en una comunidad.
  - En el mundo de la música ,podría permitir a los músicos publicar su trabajo como NFT, en forma de ediciones limitadas.
  - El jugador de la NBA Spencer Dinwiddie tokenizó su contrato para que otros pudieran invertir en él.
  - Dominios descentralizados

NFT

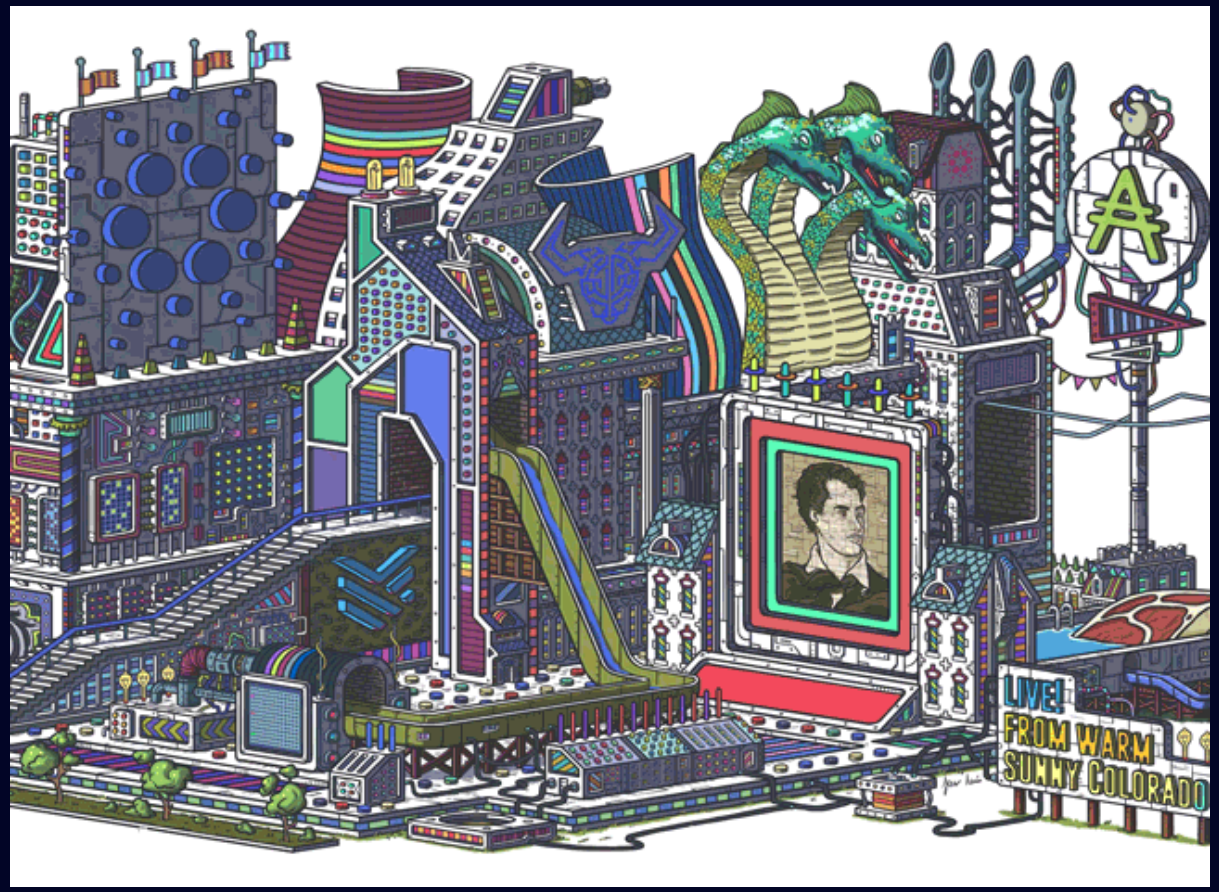
Token No Fungibles - Usos

NFT

Token No Fungibles - Usos

NFT

Token No Fungibles - Usos



NFT

Plataformas mas famosas de compra-venta de NFTs

- OpenSea
- Mintable
- Ethernity
- Valuables
- Foundation
- KnownOrigin
- SuperRare
- Nifty Gateway

OpenSea

Metaverso

El metaverso es una realidad virtual en la que interactuamos utilizando la tecnología, que, a su vez, se utiliza como puente entre la realidad física y esta nueva realidad digital

El metaverso es una combinación de numerosas tecnologías que incluyen:

- La realidad virtual
- La realidad aumentada
- Seguimiento ocular
- Blockchain
- Inteligencia artificial

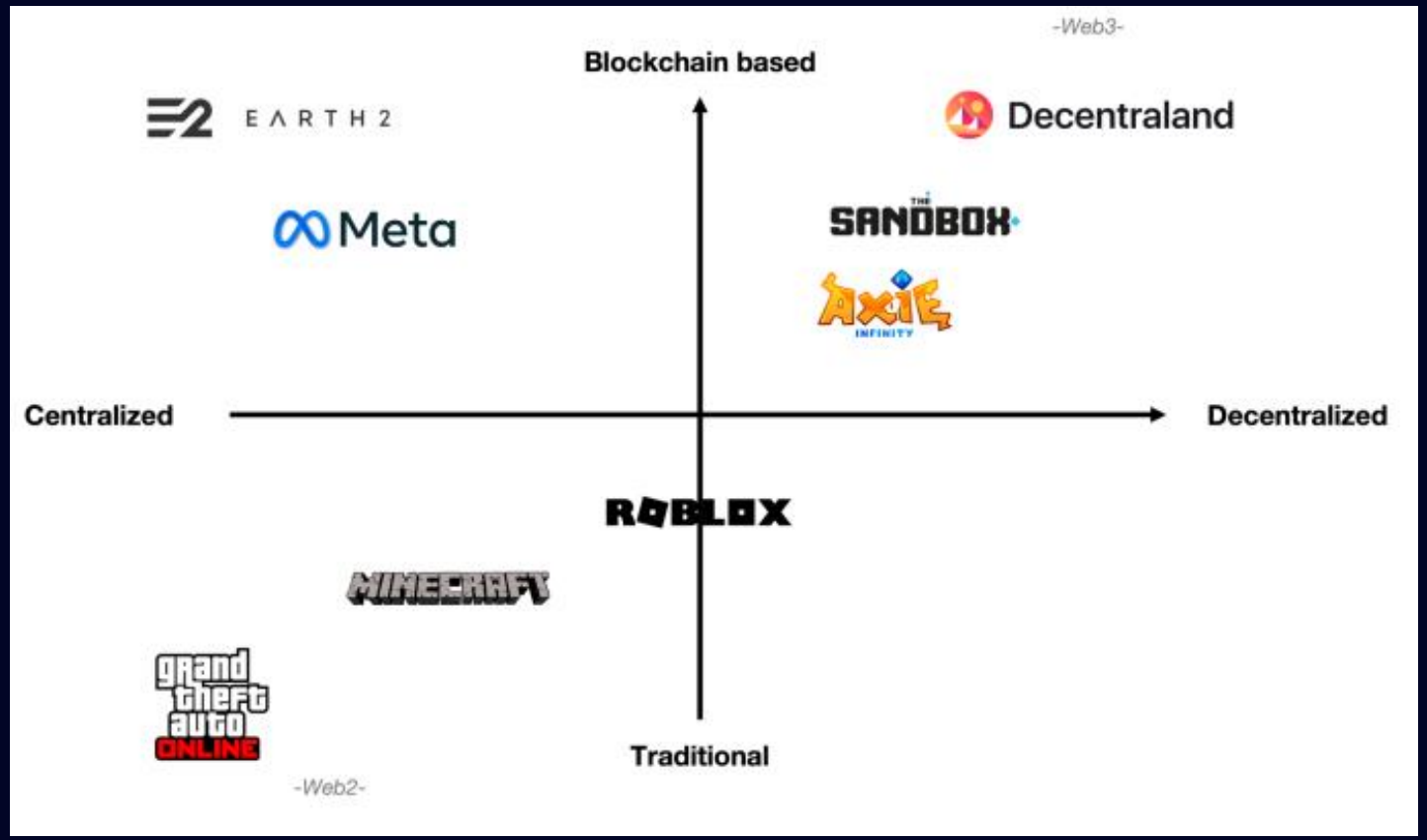
Metaverso

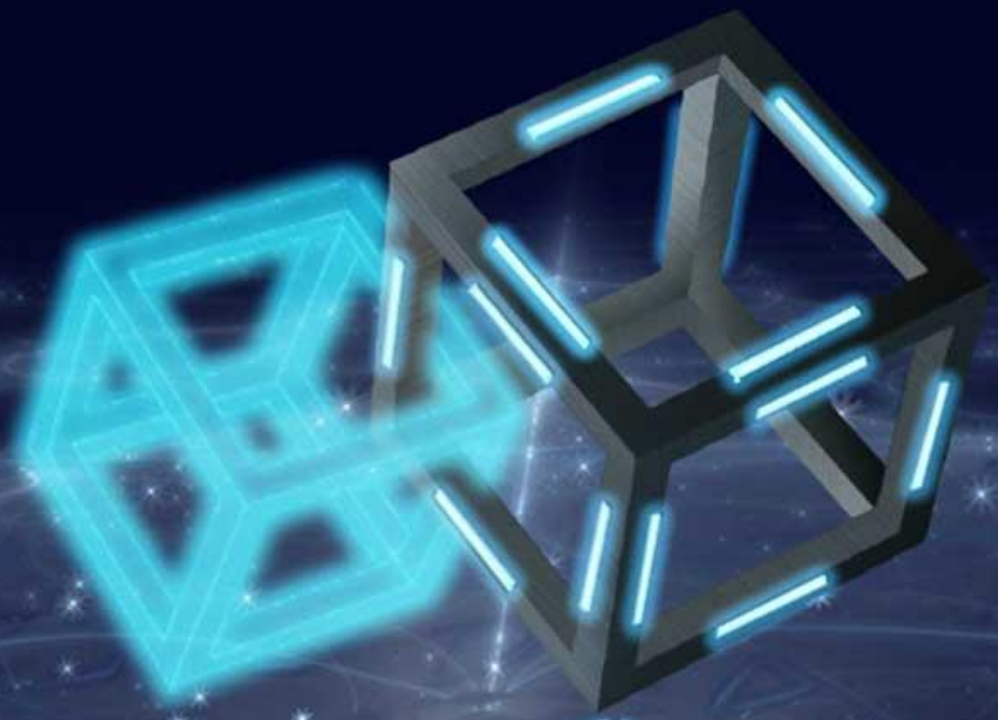
La tecnología Blockchain ha añadido un gran potencial a las aplicaciones financieras descentralizadas y a las funciones NFT, mientras que la inteligencia artificial y la realidad virtual y aumentada han añadido una experiencia de usuario sin precedentes

Podemos encontrar dos visiones del metaverso, una abierta y comunitaria, propia de los metaversos de blockchain, y otra cerrada y empresarial, como la de Microsoft o Meta, actualmente en desarrollo

Metaverso

Tipos de Metaverso





¡Gracias!