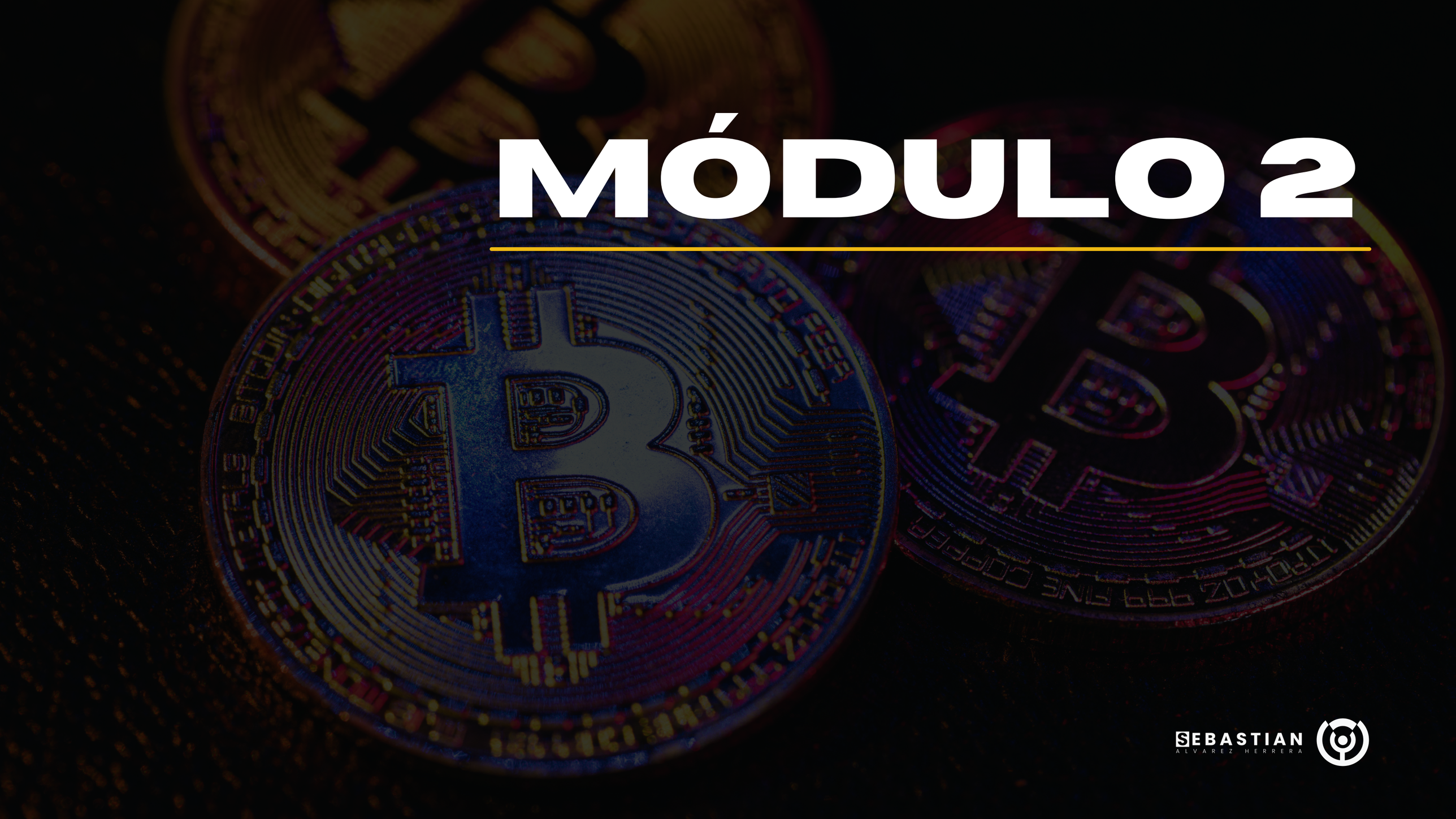
MÓDULO 2



SEBASTIAN
ALVAREZ HERRERA

MINERÍA DIGITAL

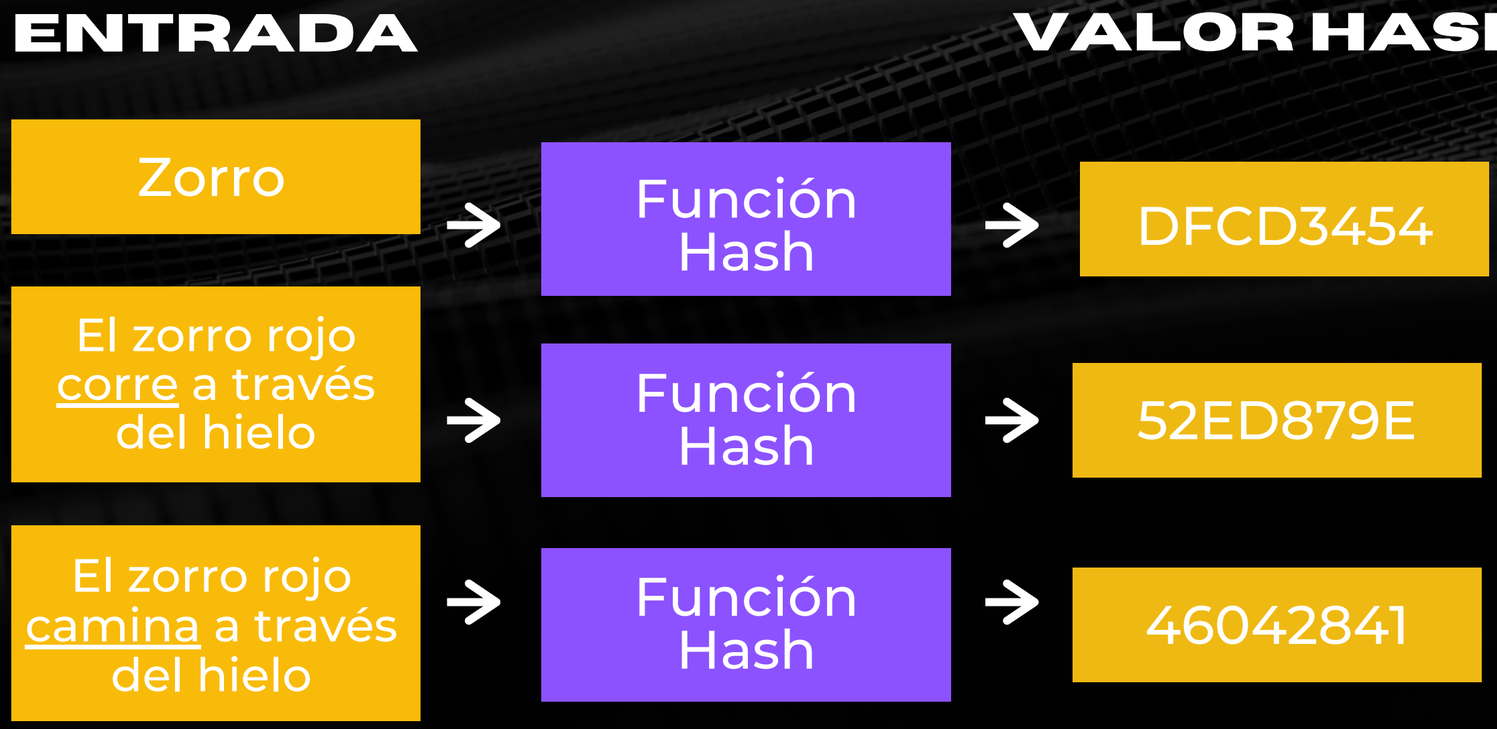
SEBASTIAN
ALVAREZ HERRERA

¿QUÉ ES LA MINERÍA DE CRIPTOMONEDAS?

La minería de criptomonedas es uno de los elementos claves que permiten que las criptomonedas funcionen como una red descentralizada de igual a igual sin la necesidad de una autoridad central de terceros. Es un proceso en el que las transacciones entre usuarios se verifican y se agregan al libro público de blockchain y también un proceso que se utiliza para introducir nuevas monedas en el suministro circulante existente.

SEBASTIAN
ALVAREZ HERRERA

FUNCIÓN HASH



SEBASTIAN
ALVAREZ HERRERA

DIFICULTAD

El término “dificultad” se emplea como una unidad de medida en el proceso de minería en criptomonedas, haciendo referencia a cómo de difícil es encontrar el hash del bloque. ... Cada bloque dentro de la red se genera a un ritmo determinado por el protocolo de la blockchain.

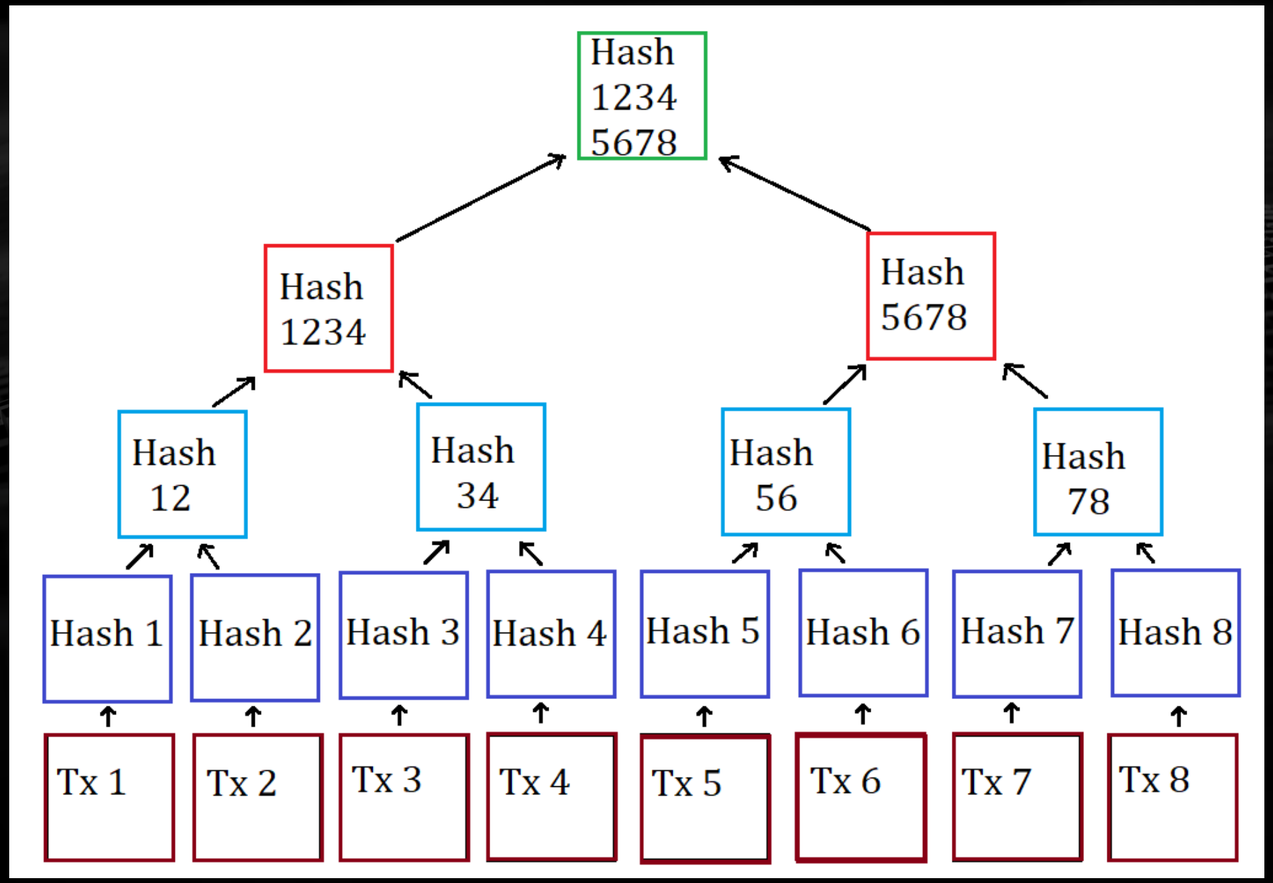
SEBASTIAN
ALVAREZ HERRERA

HASH RATE

El hash rate hace referencia a la potencia de cálculo de un minero de criptomonedas para brindar soluciones en función a un hash criptográfico en específico

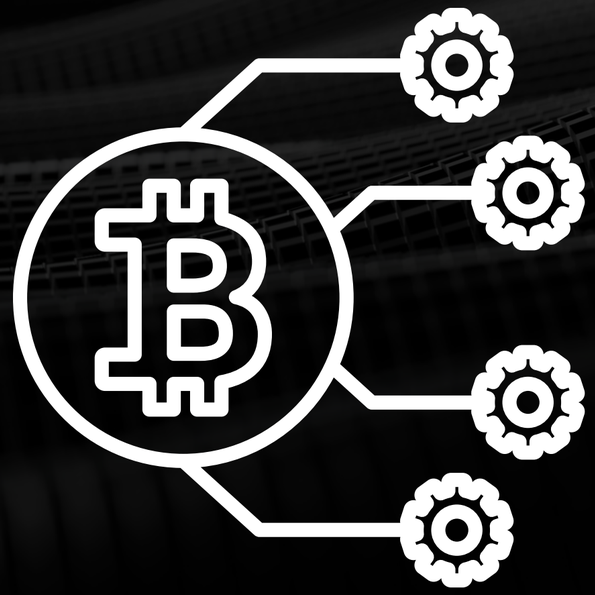
SEBASTIAN
ALVAREZ HERRERA

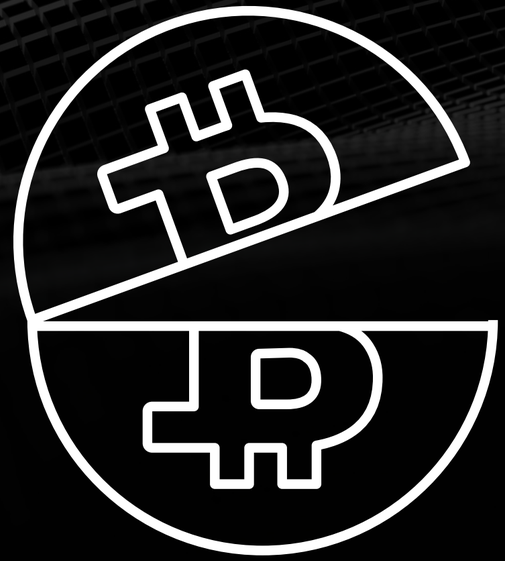
ÁRBOL DE MERKLE



SEBASTIAN
ALVAREZ HERRERA

INCENTIVOS Y ESCASEZ





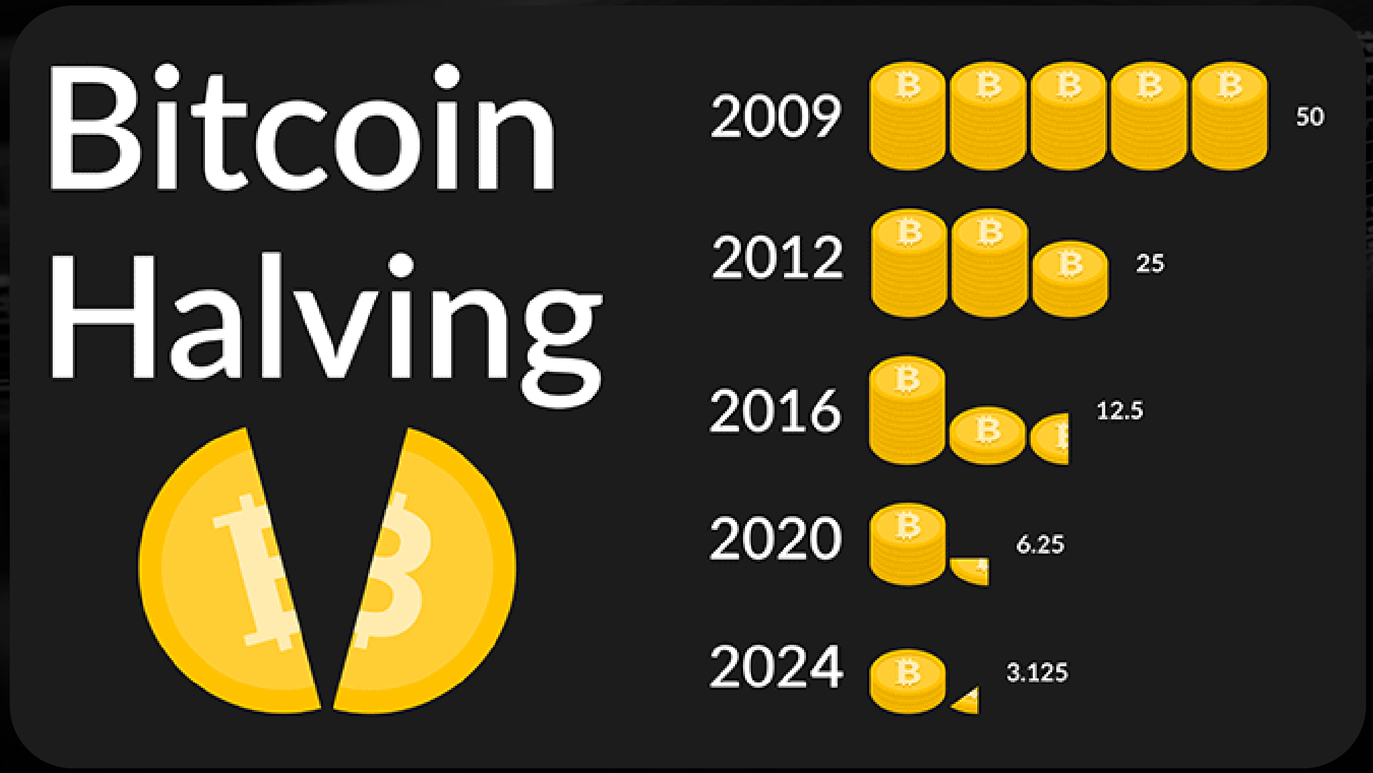
SEBASTIAN
ALVAREZ HERRERA

INCENTIVO

Por convención, la primera transacción en el bloque es una transacción especial que comienza una moneda nueva cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial de distribuir monedas en circulación, dado que no hay una autoridad para crearlas. Esta adición estable de una cantidad constante de monedas nuevas es análoga a mineros de oro gastando recursos para agregar oro a la circulación. En nuestro caso, es el tiempo del CPU y la electricidad que se gasta.

SEBASTIAN
ALVAREZ HERRERA

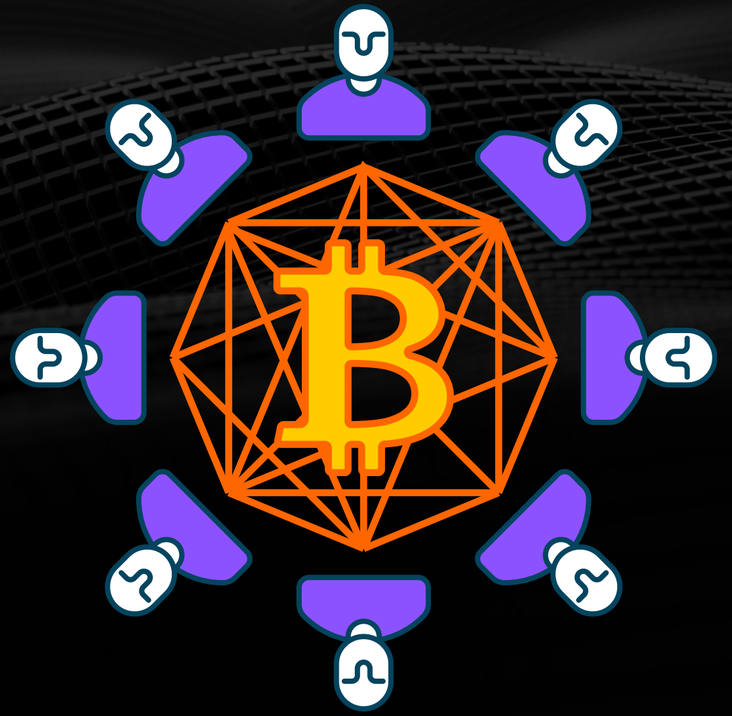
Escasez



SEBASTIAN
ALVAREZ HERRERA

POOL DE MINERÍA

Una pool de minería es un espacio que le permite a los mineros trabajar de forma cooperativa para poder minar bloques de criptomonedas.



SEBASTIAN
ALVAREZ HERRERA

BLOCKCHAIN

SEBASTIAN
ALVAREZ HERRERA

¿QUÉ ES?

La blockchain (o cadena de bloques en español), es una tecnología que permite crear un libro de contabilidad distribuida en una red de ordenadores sin necesidad de contar con un servidor o base de datos central. La actualización y manejo de este libro de contabilidad, solo se puede realizar en consenso con todas las partes que forman la red.

SEBASTIAN
ALVAREZ HERRERA

¿CÓMO SE CONSTRUYE UNA BLOCKCHAIN?

SEBASTIAN
ALVAREZ HERRERA

TIPOS DE BLOCKCHAIN

En la actualidad existen distintos tipos de blockchain cada una con sus capacidades y características únicas que se adaptan a distintas necesidades. Estos tipos de blockchain son la pública, la privada y la híbrida o federada.

SEBASTIAN
ALVAREZ HERRERA

RED BLOCKCHAIN

pública vs privada

Blockchain pública: Sin permiso
Un sistema de red abierta donde todos los dispositivos pueden acceder libremente sin ningún tipo de permiso. El registro es compartido y transparente.

Blockchain privada: Con permiso
Un usuario debe estar autorizado por la autoridad de blockchain antes de poder acceder a la red. El usuario puede unirse solo si recibe una invitación.

SEBASTIAN
ALVAREZ HERRERA

RED PÚBLICA

Este fue el primer tipo de blockchain que existió, y se refiere a las blockchains que se encuentran públicamente accesible desde Internet. Un ejemplo de este tipo de blockchain son Bitcoin, Ethereum, Dash, Monero o Zcash. Este tipo de blockchain mantienen abierto al público sus datos, el software y su desarrollo, de forma que cualquier persona puede revisar, auditar, desarrollar o mejorar los mismos.

SEBASTIAN
ALVAREZ HERRERA

RED PRIVADA O PERMISIONADA

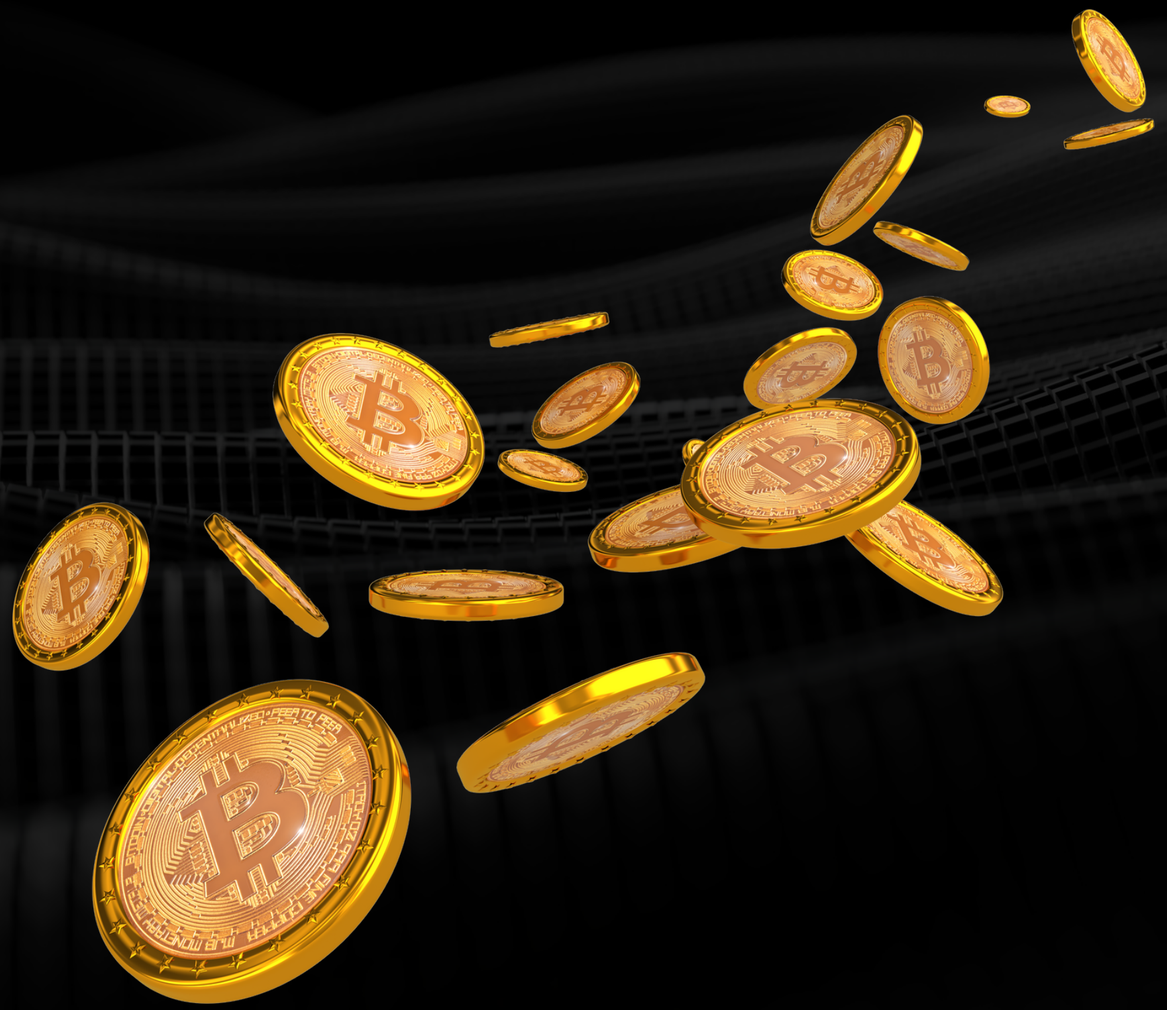
Más tarde, con la evolución de la tecnología blockchain y su expansión, muchas empresas se vieron interesadas en ella. Esto derivó en el desarrollo de soluciones blockchain privadas o permisionadas. Este tipo de blockchain generalmente cuenta con los mismos elementos que una blockchain pública, pero a diferencia de éstas, las blockchain permisionadas dependen de una unidad central que controla todas las acciones dentro de la misma.

SEBASTIAN
ALVAREZ HERRERA

BLOCKCHAIN HÍBRIDA O FEDERADA

Este tipo de blockchain es una fusión entre las blockchain públicas y las privadas. Es un intento de aprovechar lo mejor de ambos mundos. En estas blockchain, la participación en la red es privada. Es decir, el acceso a los recursos de la red es controlado por una o varias entidades. Sin embargo, el libro de contabilidad es accesible de forma pública. Esto significa que cualquier persona puede explorar bloque a bloque todo lo que sucede en dicha blockchain.

SEBASTIAN
ALVAREZ HERRERA



BITCOIN

SEBASTIAN
ALVAREZ HERRERA

¿QUÉ ES BITCOIN?

Bitcoin es la primera implementación de un concepto conocido como "moneda criptográfica", la cual fue descrita por primera vez en 1998 por Wei Dai en la lista de correo electrónico "cypherpunks", donde propuso la idea de un nuevo tipo de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada. La primera especificación del protocolo Bitcoin y la prueba del concepto la publicó Satoshi Nakamoto en el 2009 en una lista de correo electrónico. Satoshi abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo Bitcoin.

SEBASTIAN
ALVAREZ HERRERA