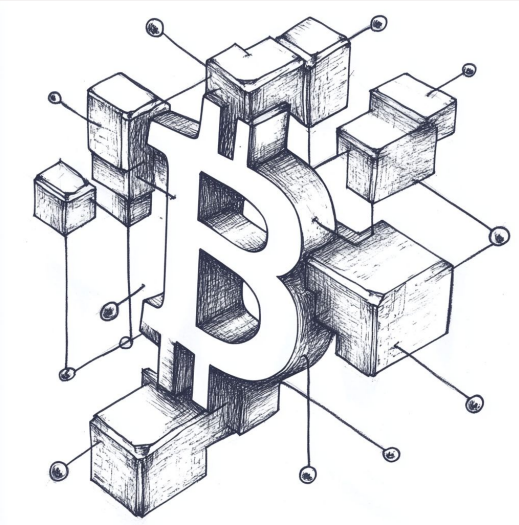
Sobre Mí

Ingeniero en computación
En Blockchain desde el 2013
Creador de meetup de blockchain Montevideo
Fundador y CEO de Infuy
Co-Fundador de ZirconTech
Referente blockchain en la CUTI

Hobbies

Jugar con mis hijas,
Arte, Carpinteria, Esqui.

INTRODUCCION A BLOKCHAIN



Alejandro Narancio
ale.narancio@gmail.com
@anarancio

Agenda

Características principales

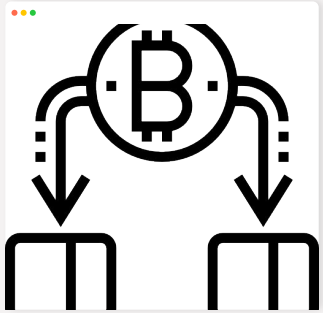
Algoritmos criptográficos

Otras características

Estructura de un bloque

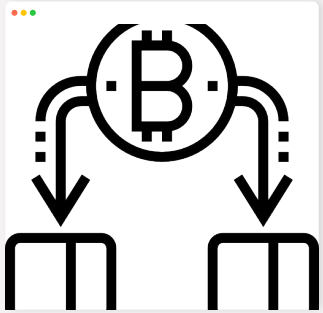
Conceptos básicos de algoritmos de consenso

Características principales



Base de datos orientada a transacciones

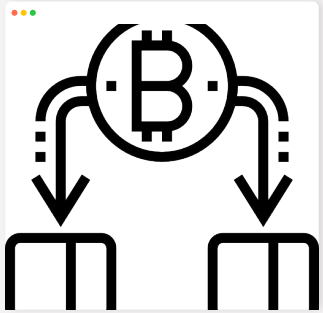
Características principales



Base de datos orientada a transacciones

DLT (Distributed Ledger Technology)

Características principales



Base de datos orientada a transacciones

DLT (Distributed Ledger Technology)

Acuerdos descentralizados

Características principales

Inmutabilidad

Características principales

Inmutabilidad

Escasez digital

Características principales

Inmutabilidad

Escasez digital

Aumento de confianza

Criptografía

HASHES

Criptografía

https://colab.research.google.com/drive/1XIJTipyS0OpAfNYOx0_xjEcIjlJdoAxz#scrollTo=ymc1uXV9CpN4

HASHES

Criptografía

HASHES

Integridad de Datos
Cualquier cambio aunque sea el más mínimo (de un bit) provocará un hash completamente distinto

Criptografía

HASHES

Integridad de Datos
Cualquier cambio aunque sea el más mínimo (de un bit) provocará un hash completamente distinto

Referencia a Bloques
Los bloques se referencian por medio de los hashes, esto provoca que el último bloque de la cadena comparta información con el primer bloque de la misma

Criptografía

HASHES

Integridad de Datos
Cualquier cambio aunque sea el más mínimo (de un bit) provocará un hash completamente distinto

Referencia a Bloques
Los bloques se referencian por medio de los hashes, esto provoca que el último bloque de la cadena comparta información con el primer bloque de la misma

PoW (Proof of Work)
Algoritmo utilizado para resolver el algoritmo de PoW de Bitcoin

Criptografía

HASHES

Integridad de Datos
Cualquier cambio aunque sea el más mínimo (de un bit) provocará un hash completamente distinto

Referencia a Bloques
Los bloques se referencian por medio de los hashes, esto provoca que el último bloque de la cadena comparta información con el primer bloque de la misma

PoW (Proof of Work)
Algoritmo utilizado para resolver el algoritmo de PoW de Bitcoin

Merkle Trees
Utilizado para resumir o referenciar todas las transacciones de un bloque en su header

Criptografía

HASHES

Integridad de Datos
Cualquier cambio aunque sea el más mínimo (de un bit) provocará un hash completamente distinto

Referencia a Bloques
Los bloques se referencian por medio de los hashes, esto provoca que el último bloque de la cadena comparta información con el primer bloque de la misma

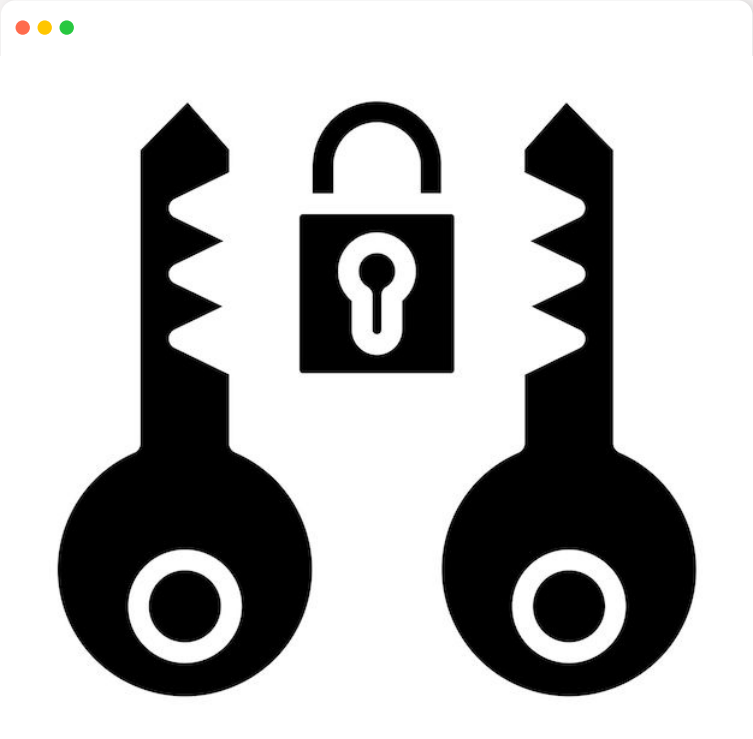
PoW (Proof of Work)
Algoritmo utilizado para resolver el algoritmo de PoW de Bitcoin

Merkle Trees
Utilizado para resumir o referenciar todas las transacciones de un bloque en su header

Firma digital

Criptografía

Algoritmos Asimétricos

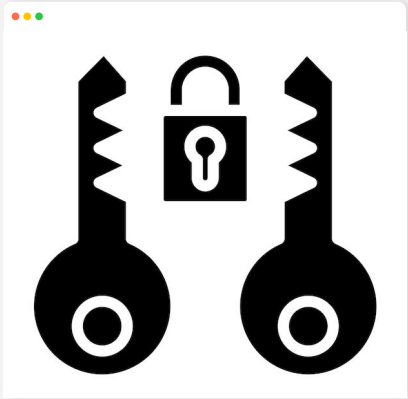


Criptografía

Algoritmos Asimétricos

Criptografía

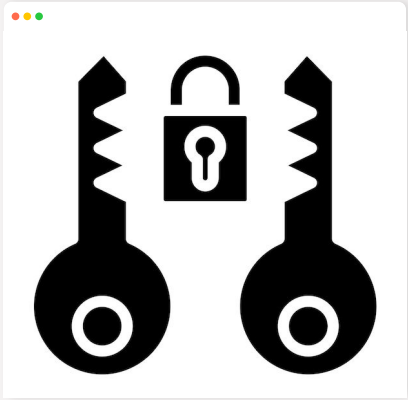
Algoritmos Asimétricos



Firmas digitales
Todas las transacciones son firmadas con la clave privada de una cuenta

Criptografía

Algoritmos Asimétricos

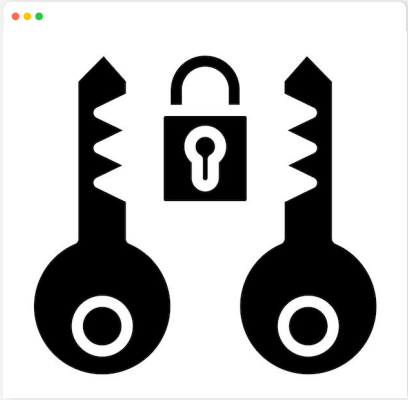


Firmas digitales
Todas las transacciones son firmadas con la clave privada de una cuenta

Generaciones de direcciones (address) de billeteras
Una billetera posee por atrás al menos una clave privada

Criptografía

Algoritmos Asimétricos



Firmas digitales
Todas las transacciones son firmadas con la clave privada de una cuenta

Generaciones de direcciones (address) de billeteras
Una billetera posee por atrás al menos una clave privada

Validación y consenso
Durante las reglas de consenso una de las validaciones serán las firmas digitales utilizando las claves públicas

Criptografía

Firma Digital

Criptografía

Firma Digital

Autenticación
Se puede validar que el emisor del mensaje es realmente quien dice ser.

Criptografía

Firma Digital

Autenticación
Se puede validar que el emisor del mensaje es realmente quien dice ser.

No repudio
El emisor del mensaje no puede negar que el lo emitió

Criptografía

Firma Digital

Autenticación
Se puede validar que el emisor del mensaje es realmente quien dice ser.

No repudio
El emisor del mensaje no puede negar que el lo emitió

Integridad
Se garantiza que el mensaje es exactamente el que quiso enviar el emisor y no fue modificado

Criptografía

Firma Digital

Alice

Criptografía

Firma Digital

Alice

Clave privada de Alice (PrivKa)

Clave pública de Alice (PubKa)

Criptografía

Firma Digital (firma)

Alice

Documento a firmar

Criptografía

Firma Digital (firma)

Alice

Documento a firmar

HASH

Hash (fingerprint) del documento

Criptografía

Firma Digital (firma)

Alice

Documento a firmar

HASH

Hash (fingerprint) del documento

Clave privada de Alice

Firma digital del hash del documento

Criptografía

Firma Digital

Alice

Documento

Firma digital del hash del documento

Alice envía a Bob

Documento

Firma digital del hash del documento

Bob

Criptografía

Firma Digital (verificación)

Bob

Documento

Firma digital del hash del documento

Criptografía

Firma Digital (verificación)

Bob

Documento

HASH

Hash (fingerprint) del documento

Firma digital del hash del documento

Criptografía

Firma Digital (verificación)

Bob

Documento

HASH

Hash (fingerprint) del documento

Firma digital del hash del documento

Clave pub de Alice

Hash (fingerprint) del documento

Criptografía

Firma Digital (verificación)

Bob

Documento

HASH

Hash (fingerprint) del documento

COMPARACIÓN

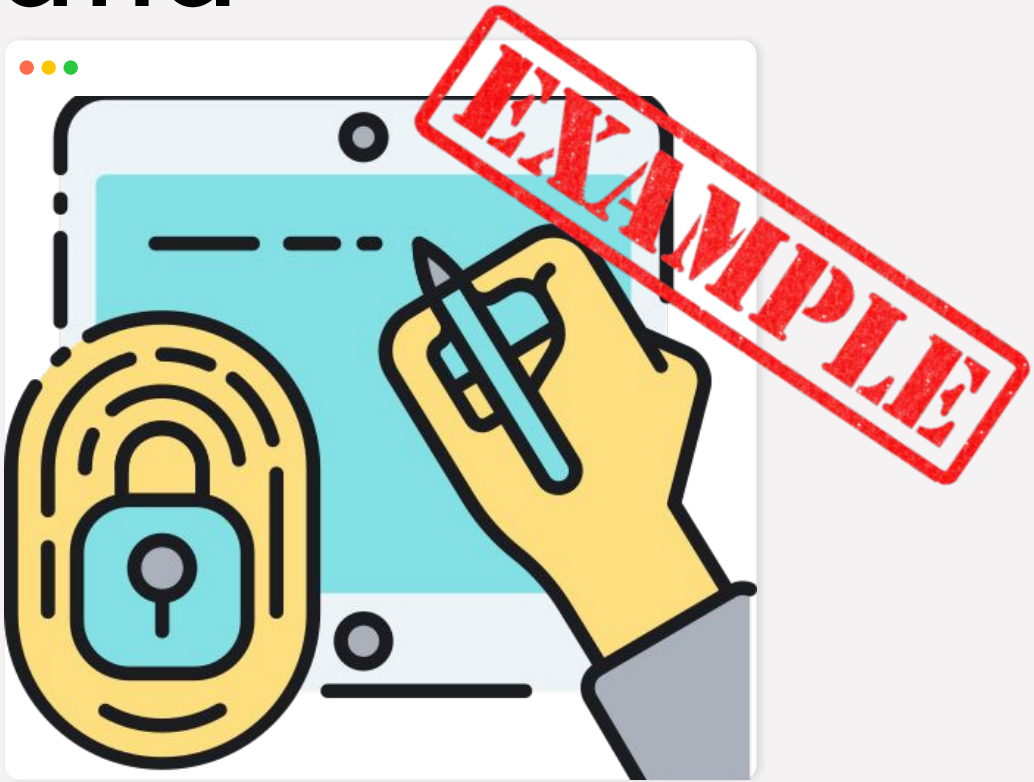
Firma digital del hash del documento

Clave pub de Alice

Hash (fingerprint) del documento

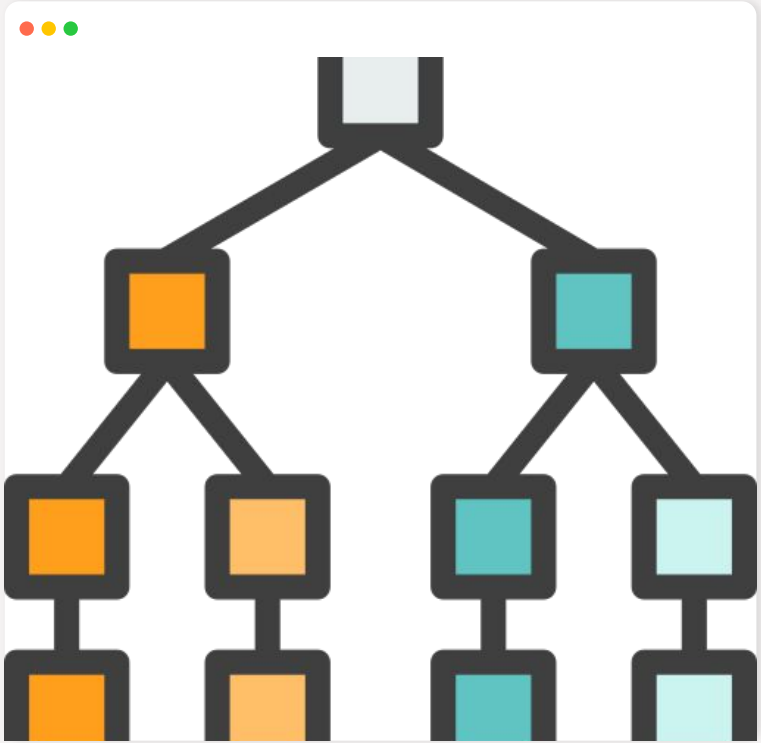
Criptografía

Firma Digital



Criptografía

Merkle Trees

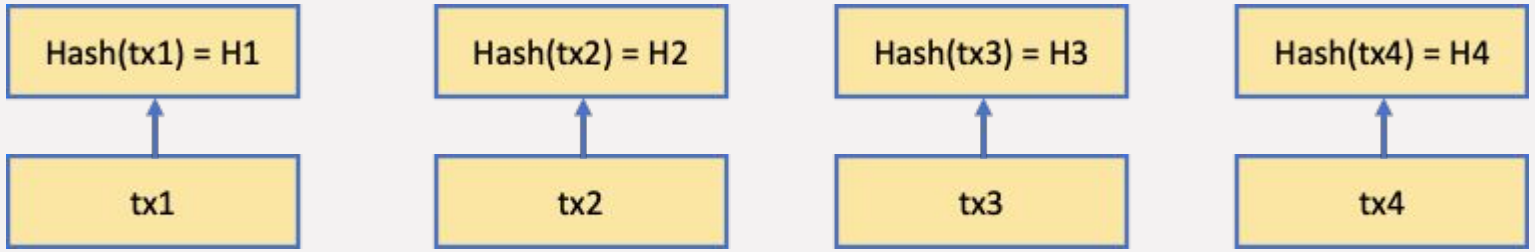


Criptografía

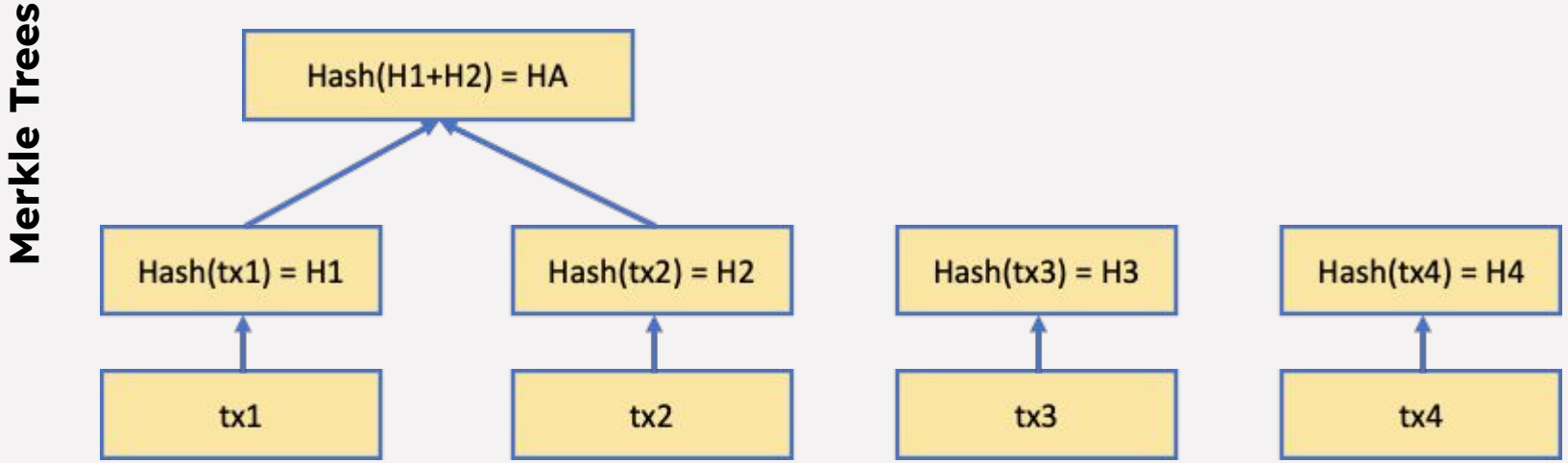
Merkle Trees

Criptografía

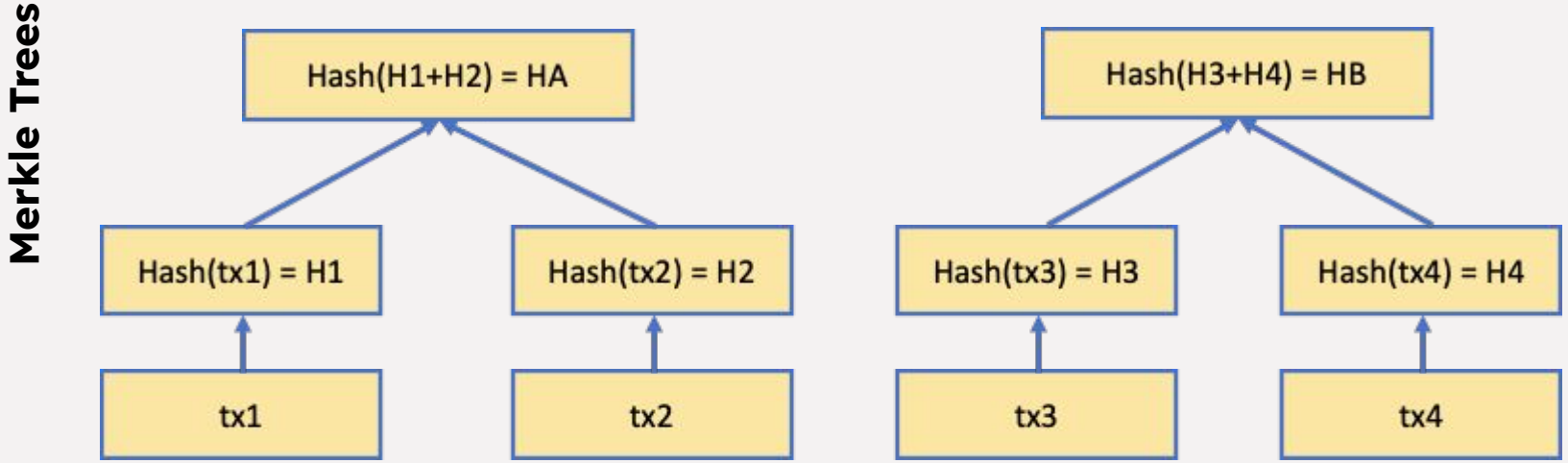
Merkle Trees



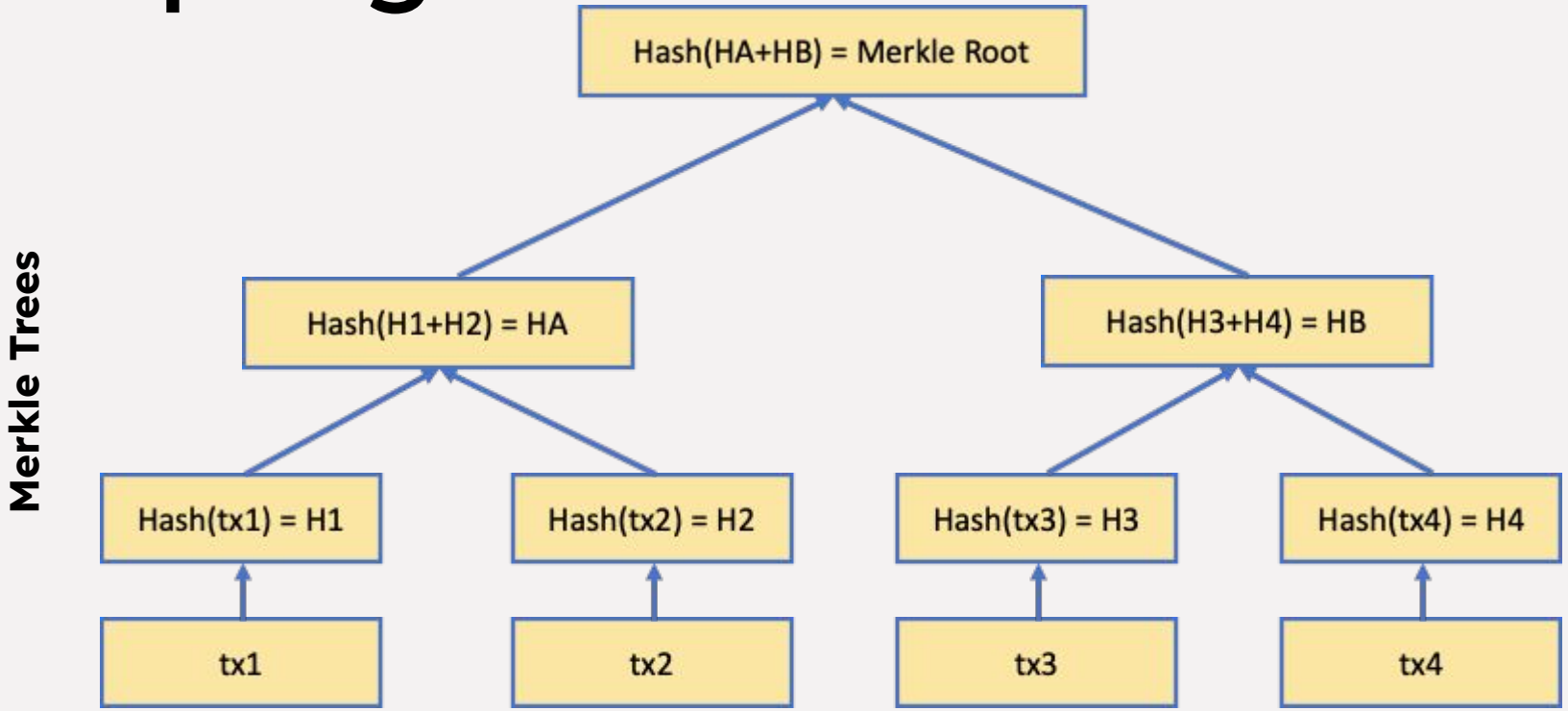
Criptografía



Criptografía



Criptografía

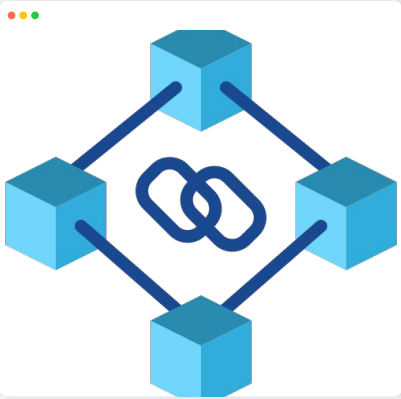


Criptografía

Merkle Trees

Otras características

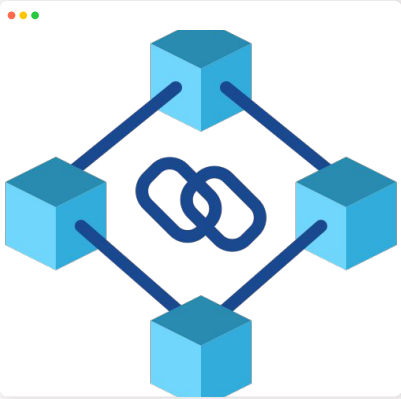
Blockchain



Orientado a transacciones
Cada vez que se realiza una acción se crea una transacción

Otras características

Blockchain

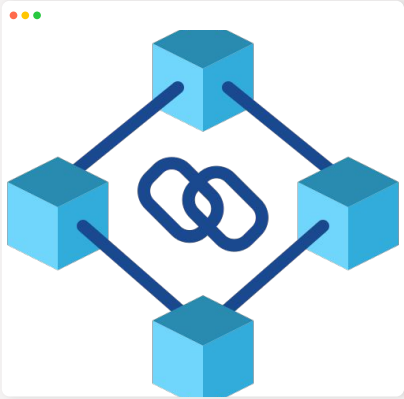


Orientado a transacciones
Cada vez que se realiza una acción se crea una transacción

Bloques
Las transacciones se agrupan en bloques

Otras características

Blockchain



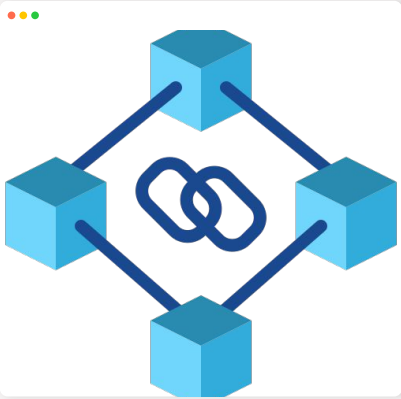
Orientado a transacciones
Cada vez que se realiza una acción se crea una transacción

Bloques
Las transacciones se agrupan en bloques

Referencia al bloque anterior
Cada bloque (excepto el genesis) posee una referencia al bloque anterior, formando una cadena

Otras características

Blockchain



Orientado a transacciones
Cada vez que se realiza una acción se crea una transacción

Bloques
Las transacciones se agrupan en bloques

Referencia al bloque anterior
Cada bloque (excepto el genesis) posee una referencia al bloque anterior, formando una cadena

Unico camino al genesis
Desde cualquier bloque de la cadena solo existe un camino hacia el génesis block

Estructura básica de un bloque

Bloque

HEADER

(número de bloque, hash bloque anterior, timestamp, otros campos)

Estructura básica de un bloque

Bloque

HEADER

(número de bloque, hash bloque anterior, timestamp, otros campos)

DATOS

Estructura básica de un bloque

Bloque

HEADER

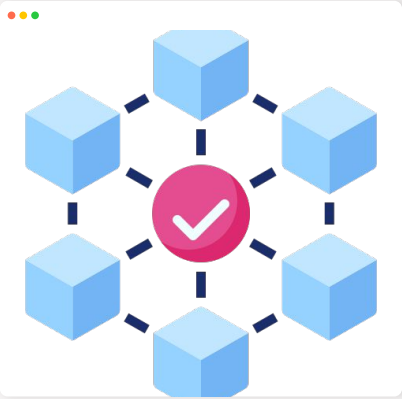
(número de bloque, hash bloque anterior, timestamp, otros campos)

DATOS

FIRMA DIGITAL

Algoritmos de consenso

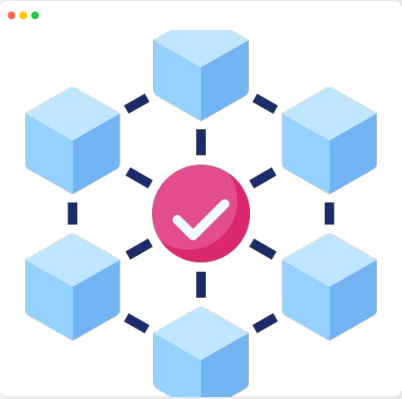
Consenso



Para qué sirven?
Permite a un grupo diverso tomar decisiones

Algoritmos de consenso

Consenso

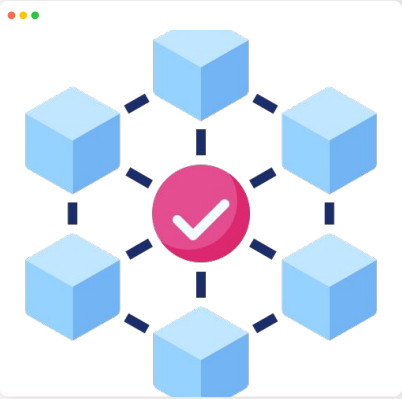


Para qué sirven?
Permite a un grupo diverso tomar decisiones

Características necesarias
Se requiere que todos los participantes acepten las mismas reglas y reconocen que todos son iguales respecto al consenso

Algoritmos de consenso

Consenso



Para qué sirven?
Permite a un grupo diverso tomar decisiones

Características necesarias
Se requiere que todos los participantes acepten las mismas reglas y reconocen que todos son iguales respecto al consenso

Ejemplos
PoW, PoS, DPoS, etc.