Introducción a la Codificación y Encriptación

La codificación y encriptación son conceptos fundamentales en la informática moderna. La codificación se refiere a la representación de información en un formato digital. La encriptación, por otro lado, es el proceso de convertir información en un formato ilegible sin la clave correcta.

by **KEVIN STEVE MARTÍNEZ LEMUS**

Conceptos básicos de la codificación

1 Conversión de datos

La codificación traduce información, como texto o imágenes, a un formato que las computadoras pueden procesar.

2 Sistemas de Codificación

Existen varios sistemas de codificación, como ASCII, Unicode y UTF-8, cada uno con sus propias características y ventajas.

3 Eficiencia

La codificación permite un uso eficiente del almacenamiento y la transmisión de información.

Tipos de algoritmos de encriptación

Encriptación simétrica

Utiliza la misma clave para cifrar y descifrar datos. Es rápida y eficiente, pero requiere que ambas partes compartan la clave.

Encriptación asimétrica

Utiliza dos claves diferentes, una pública y otra privada. La clave pública se utiliza para cifrar datos, mientras que la privada se utiliza para descifrarlos.

Funciones hash

Generan una huella digital única para los datos, asegurando su integridad y autenticidad. Son unidireccionales, lo que significa que no se pueden revertir.

Criptografía simétrica y asimétrica

Simétrica

La clave se comparte entre el emisor y el receptor. Es eficiente, pero la seguridad depende de la protección de la clave.

Asimétrica

Utiliza dos claves, una pública y otra privada. La clave pública se puede compartir, mientras que la privada se mantiene en secreto.

Aplicaciones de la encriptación

1 Comunicación segura

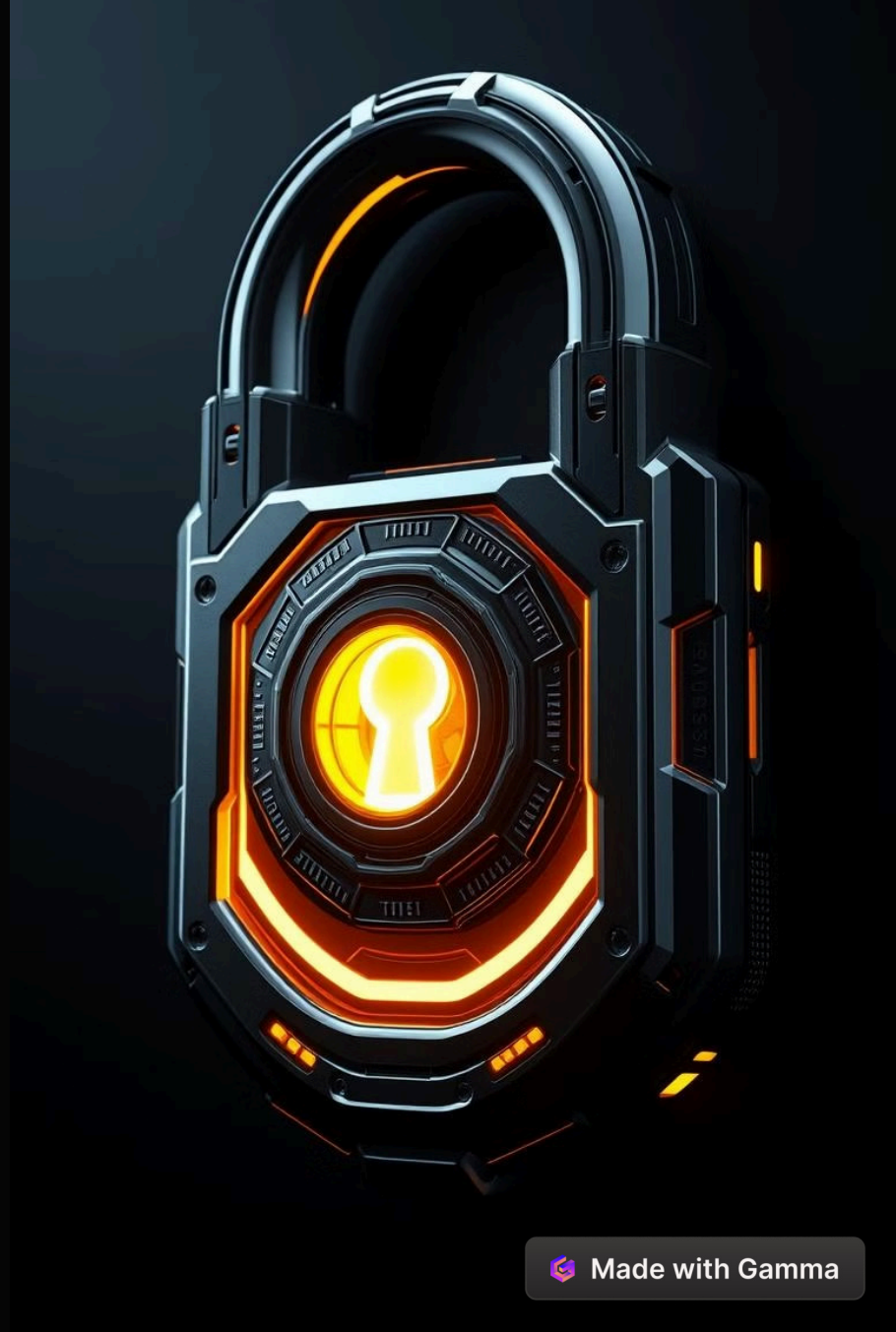
La encriptación protege las comunicaciones de las escuchas.

2 Almacenamiento de datos

La encriptación protege los datos almacenados en dispositivos y servidores.

3 Autenticación

La encriptación verifica la identidad de los usuarios y dispositivos.



¿Qué es un Árbol de Merkle?

1

Estructura de datos

Un árbol de Merkle es una estructura de datos jerárquica que almacena información hash de los datos.

2

Nodos hash

Cada nodo del árbol representa un hash de los datos o de los nodos hijos.

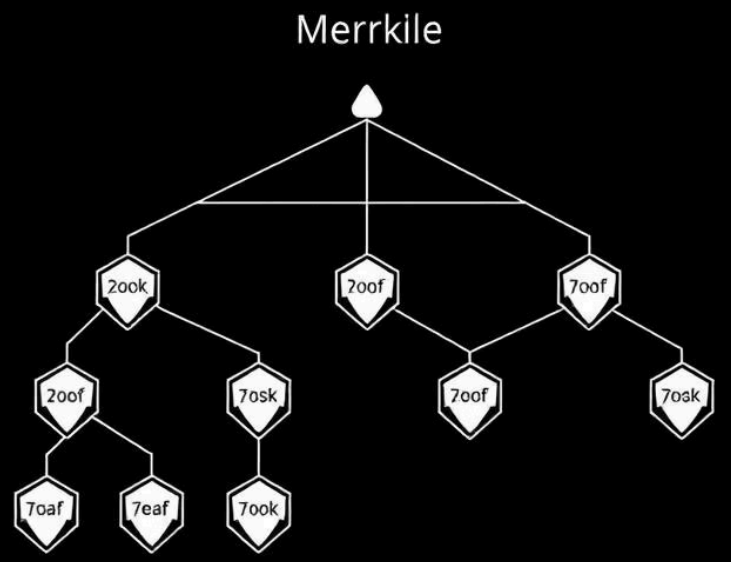
3

Raíz del árbol

La raíz del árbol contiene el hash de todos los datos del árbol.

Estructura y funcionamiento del Árbol de Merkle

Paso	Descripción
1	Los datos se dividen en bloques.
2	Se calcula un hash para cada bloque.
3	Los hashes se combinan en pares y se calcula un nuevo hash para cada par.
4	El proceso se repite hasta que solo queda un hash, la raíz del árbol.



Ventajas del Árbol de Merkle en blockchain

Verificación de datos

Los árboles de Merkle permiten verificar la integridad de los datos en una blockchain de forma eficiente.

Eficiencia

Los árboles de Merkle reducen la cantidad de datos que se necesitan descargar para verificar la integridad.

Seguridad

Los árboles de Merkle dificultan la manipulación de datos en una blockchain.

Seguridad en blockchain

1

Criptografía

La criptografía se utiliza para asegurar las transacciones y proteger los datos.

2

Consenso distribuido

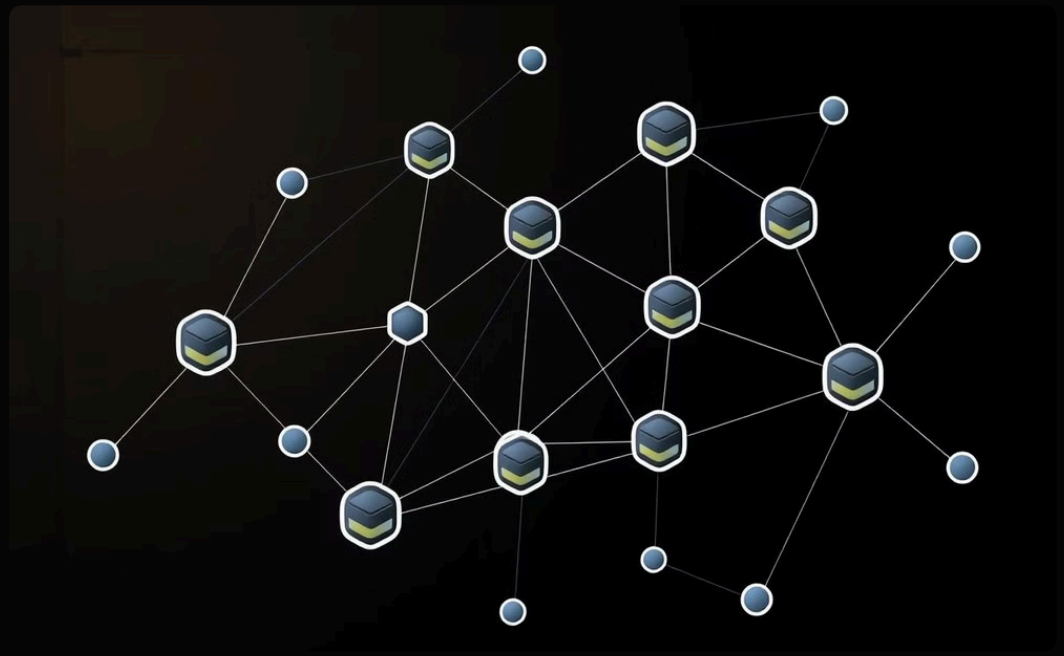
Todos los nodos en la red deben estar de acuerdo en la validez de las transacciones.

3

Inmutabilidad

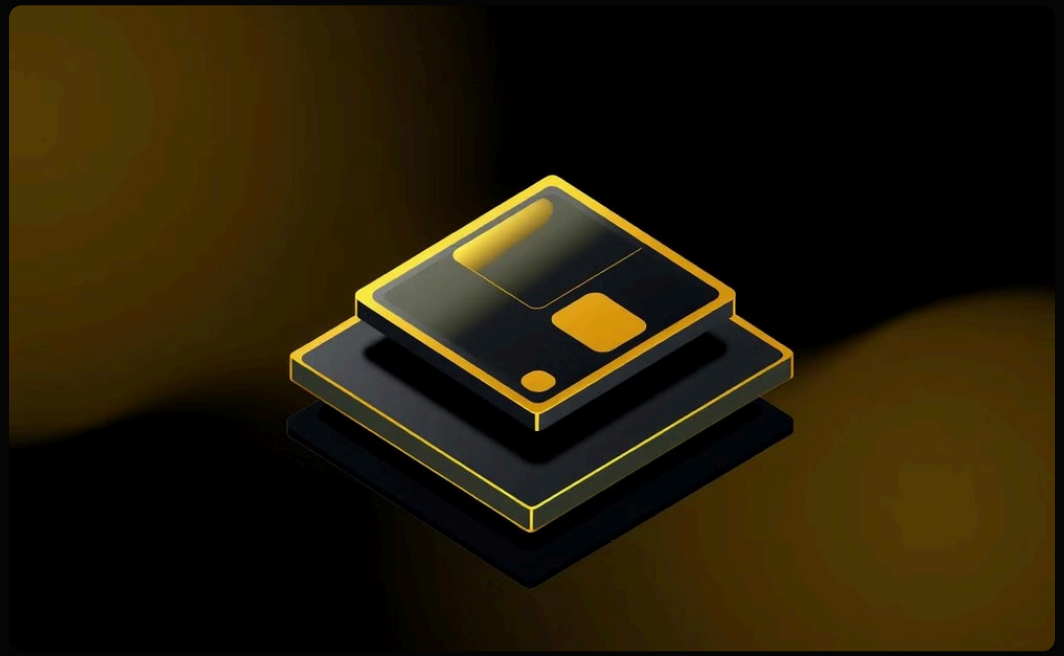
Los datos en una blockchain son inmutables, lo que significa que no se pueden modificar una vez que se registran.

Eficiencia y escalabilidad en blockchain



Paralelismo

Las transacciones se pueden procesar en paralelo en múltiples nodos.



Escalabilidad horizontal

La red se puede ampliar agregando más nodos para manejar más transacciones.