COLOMBIA POTENCIA DE LA VIDA

TIC

Historia y **desarrollo de blockchain**

Lección 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Tiempo de ejecución: 6 horas

PLANTEAMIENTO DE LA SESIÓN	Materiales
En la segunda sesión se expondrá la historia del blockchain, sus orígenes y las tecnologías que se implementaron para su desarrollo y funcionamiento. Al final de la sesión se propone una actividad o cuestionario de los conocimientos adquiridos en la sesión.	Bitcoin: A Peer-to-Peer Electronic Cash System: 

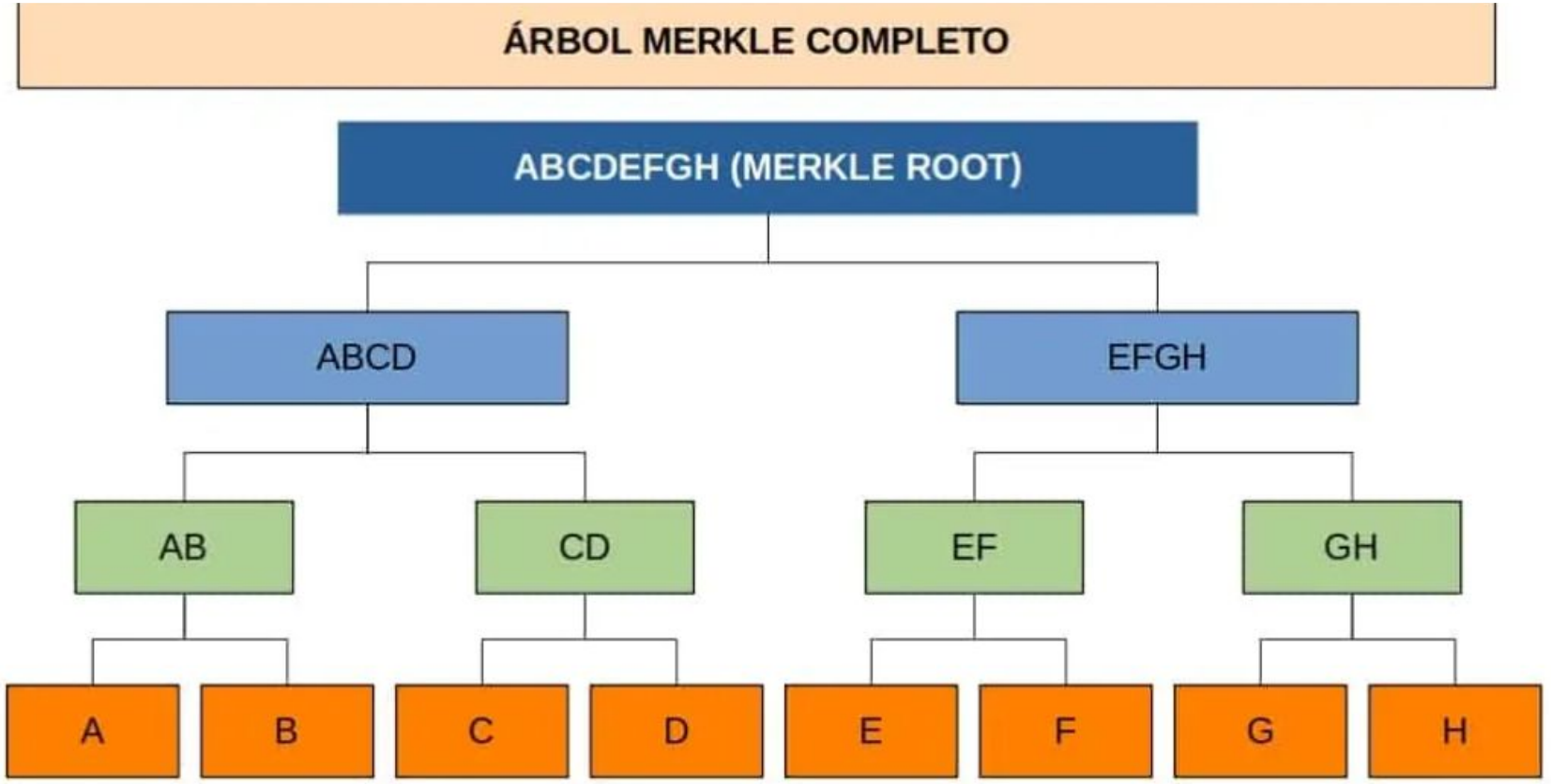
Desarrollo teórico de la sesión: 4 horas

Historia del blockchain.

En el año 1,991 los científicos de investigación Stuart Haber y W. Scott Stornetta desarrollaron una solución para los documentos digitales con sello de tiempo para que no fueran inmutables, es decir, estos documentos no podrían ser manipulados o modificados por un usuario en concreto, con esto se garantiza la integridad de la información contenida en los archivos en cuestión.

Este sistema utilizó una cadena de bloques con seguridad criptográfica para el almacenamiento de los documentos digitales con sello de tiempo. En el año 1,992 se incorpora al diseño de los árboles Merkle, estos árboles son estructuras de datos divididas en varias capas que tienen la finalidad de relacionar cada nodo con una raíz única asociada a los mismos. Cada nodo debe tener un identificador hash y la estructura va conectada como en el siguiente diagrama:

+ info


ÁRBOL MERKLE COMPLETO
ABCDEFGH (MERKLE ROOT)
ABCD
EFGH
AB
CD
EF
GH
A
B
C
D
E
F
G
H

Este diseño fue creado en 1,979 por Ralph Merkle, con el fin de optimizar el proceso de verificación de grandes cantidades de datos

Esta estructura de datos permite relacionar una gran cantidad de datos en un único punto (Merkle root), con esto, la veracidad e identificación de los datos puede ser muy eficiente al tener que verificar solo el Merkle root en vez de toda la estructura.

Sin embargo, la tecnología antes descrita no se utilizó y la patente caducó en 2,004, cuatro años antes del inicio de Bitcoin.

COLOMBIA POTENCIA DE LA VIDA

TIC

Prueba de trabajo reutilizable.

Evolución

Transacción

Tokens

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

El sistema utilizó el marco de trabajo de Hashcash, que ya había sido propuesto por Adam Back en 1997 como una medida contra el spam. La innovación clave de RPoW fue la adición de la firma RSA para crear tokens transferibles. Estos tokens podían ser transferidos de una persona a otra, permitiendo una forma temprana de transacción digital.

La Prueba de Trabajo Reutilizable (RPoW) propuesta por Hal Finney en 2004 representa un hito crucial en la evolución de las criptomonedas. En ese momento, el concepto de criptomonedas apenas estaba tomando forma, y RPoW abordó de manera innovadora el desafío del doble gasto, que había sido un problema persistente en sistemas electrónicos de efectivo.

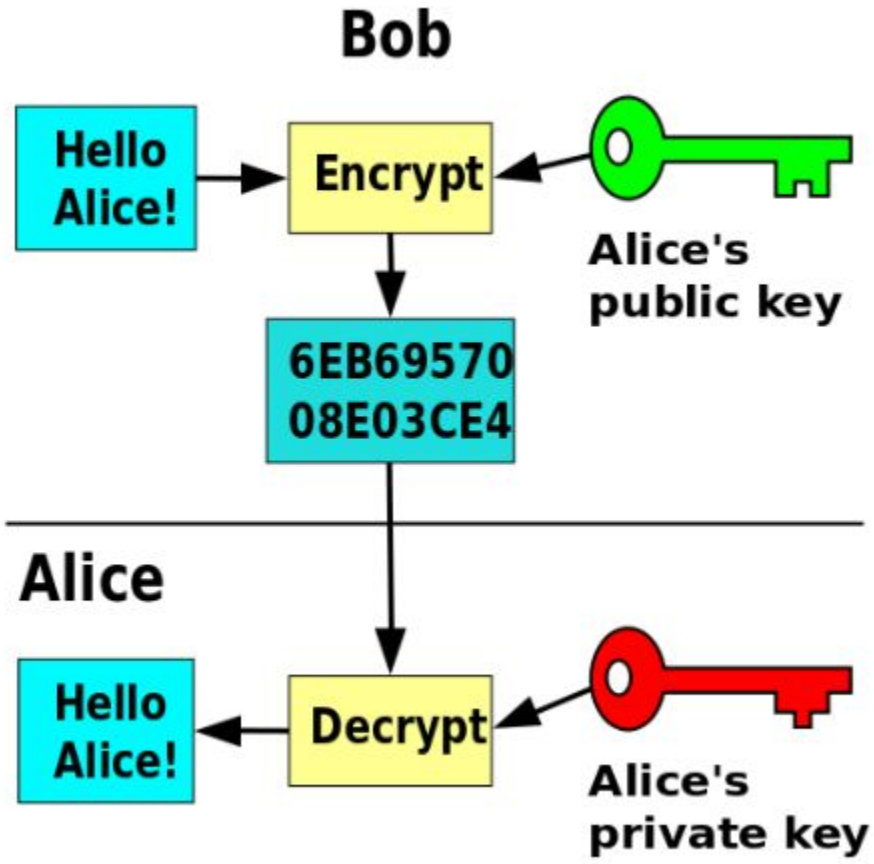
RPoW introdujo la idea de tokens no fungibles generados a través de pruebas de trabajo, lo que significa que cada token tenía un valor único y no podía intercambiarse directamente con otros tokens. Este enfoque proporcionó una forma de representar propiedad digital única y transferible.

Algoritmo RSA

Anteriormente se mencionó la firma RSA para crear tokens transferibles, pero ¿qué es RSA? Es un algoritmo de criptografía de clave pública inventado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. Utiliza un par de claves, una pública compartida y una privada secreta. La clave pública encripta mensajes, y solo la clave privada correspondiente puede desencriptarlos, asegurando la confidencialidad.

Además, RSA se emplea para crear firmas digitales, verificando la autenticidad y la integridad de los datos. La seguridad de RSA radica en la dificultad computacional de factorizar grandes números compuestos. Aunque ampliamente utilizado, su vulnerabilidad potencial a futuros avances en la factorización cuántica ha llevado a la exploración de algoritmos de criptografía cuántica como alternativas.

+ Mapa conceptual


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Red Bitcoin.

En el final de 2008, una figura enigmática o grupo bajo el seudónimo Satoshi Nakamoto presentó un documento técnico en una lista de correo de criptografía, dando origen a Bitcoin, un sistema de efectivo electrónico descentralizado entre pares. Este innovador sistema, basado en el algoritmo de Prueba de Trabajo de Hashcash, implementa un enfoque descentralizado de igual a igual para rastrear y verificar transacciones, proporcionando una doble protección contra el gasto duplicado.

En lugar de depender de un sistema confiable de hardware como RPoW, los mineros individuales utilizan el mecanismo de prueba de trabajo para "extraer" bitcoins, y las transacciones son verificadas por nodos descentralizados en la red. El 3 de enero de 2009, se minó el primer bloque de Bitcoin, marcando su nacimiento, con una recompensa de 50 bitcoins. La primera transacción de Bitcoin ocurrió el 12 de enero de 2009, donde Satoshi Nakamoto envió 10 bitcoins al pionero Hal Finney. Este hito marcó el comienzo de la era de las criptomonedas.

Creación de Ethereum.

En 2013, Vitalik Buterin, un programador y cofundador de la revista Bitcoin, planteó la necesidad de un lenguaje de scripting en Bitcoin para construir aplicaciones descentralizadas. Ante la falta de consenso en la comunidad, Vitalik emprendió el desarrollo de Ethereum, una nueva plataforma de computación distribuida basada en blockchain que incorpora funcionalidades de scripting, conocidas como contratos inteligentes.

Los contratos inteligentes son programas ejecutables en la cadena de bloques Ethereum, capaces de realizar acciones automáticamente si se cumplen ciertas condiciones. Escritos en lenguajes de programación específicos, se compilan en un código de bytes que la máquina virtual Ethereum (EVM) puede interpretar y ejecutar de manera descentralizada.

Además de los contratos inteligentes, los desarrolladores pueden crear y desplegar aplicaciones directamente en la cadena de bloques Ethereum, conocidas como aplicaciones descentralizadas (DApps). La plataforma alberga una amplia variedad de DApps, desde redes sociales hasta plataformas de juegos de azar y servicios financieros descentralizados.

En un sistema descentralizado, el control y la toma de decisiones se distribuyen entre múltiples participantes, aumentando la resistencia a fallos y reduciendo la vulnerabilidad. En contraste, en un sistema centralizado, una entidad única detenta el control, brindando eficiencia, pero siendo más propenso a fallos y manipulación

Red Bitcoin.

La criptomoneda nativa de Ethereum es Ether (ETH), que se transfiere entre cuentas y se utiliza para abonar las tarifas asociadas al procesamiento de contratos inteligentes. Este ecosistema dinámico ha contribuido significativamente a la expansión del uso de blockchain más allá de las transacciones de criptomonedas.

Desde la creación de Ethereum en 2013, la tecnología blockchain ha experimentado un rápido avance. Ethereum introdujo los contratos inteligentes, permitiendo aplicaciones descentralizadas (DApps). Posteriormente, surgieron numerosas DApps y proyectos DeFi (Finanzas Descentralizadas). La popularidad de NFTs (Tokens No Fungibles) también creció, destacando la singularidad y propiedad digital. Además, blockchain ha sido adoptado en diversas industrias para mejorar la transparencia y la eficiencia, mientras que la exploración de tecnologías como la capa 2 y la interoperabilidad continúa impulsando el desarrollo del ecosistema blockchain.