COLOMBIA POTENCIA DE LA VIDA

TIC

Módulo 1

ARQUITECTURA Y ESTRUCTURA BÁSICA DE UN BLOQUE

Lección 1 -Unidad 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Tiempo de ejecución: 4 horas

PLANTEAMIENTO DE LA SESIÓN	Materiales
En esta lección se expondrá la arquitectura y estructura básica de los bloques, sus elementos principales y las utilidades e información que contiene cada uno de ellos. Conociendo la estructura de los bloques, se comentarán las generalidades del funcionamiento de blockchain (consenso, descentralización, criptografía).	N/A

Desarrollo teórico de la sesión: 2 horas

COLOMBIA POTENCIA DE LA VIDA

TIC

Arquitectura y estructura básica de un bloque

Esto es un párrafo de Blockchain es un sistema descentralizado y distribuido, en el cual todos los participantes de una red tienen acceso a todas las transacciones que se han hecho por los demás usuarios y pueden hacer procesos de validación para garantizar la integridad de los datos en las transacciones. Todos estos usuarios tienen una copia de la cadena en tiempo real y pueden verificar si hay discrepancias en los registros con la información que está disponible en cada uno de los bloques.

Para entender su funcionamiento, primero se debe conocer su estructura y cuáles son los principales elementos que contiene cada bloque conectado en la cadena y cuál es la función de cada uno de ellos.

En la siguiente figura (Figura 1), se puede apreciar una cadena de bloques, cada uno con información específica que permite a los usuarios identificarlos de manera inequívoca.

listo para escribir un contenido genial

+imagen

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

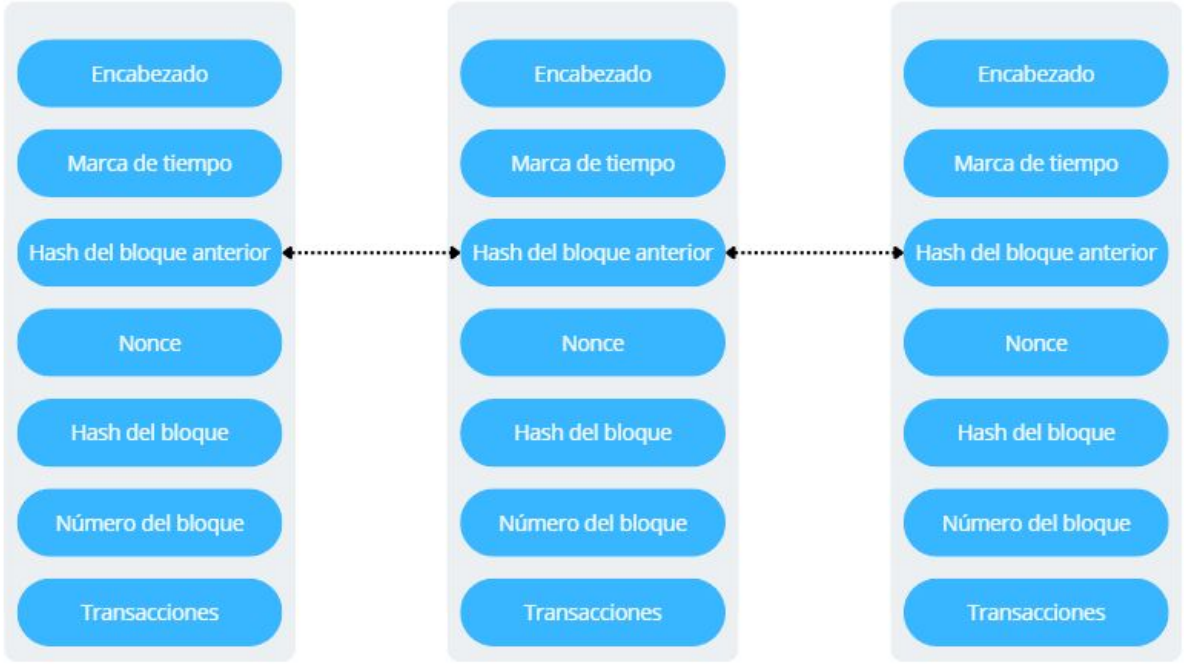
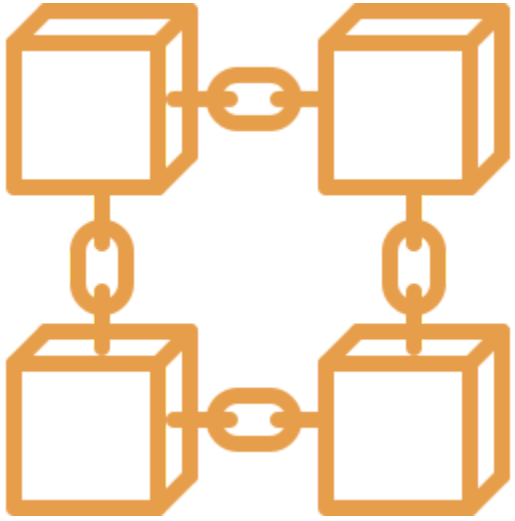


Figura 1 A continuación las definiciones de cada elemento y cómo se conecta la cadena.

- Encabezado
- Marca de tiempo
- Nonce
- Hash del bloque
- Hash del bloque anterior
- Número del bloque
- Transacciones



Hash del bloque anterior:

Cada bloque nuevo que ingresa está conectado con el último a través del hash de este, así es posible validar que una cadena no ha sido alterada, ya que, como se mencionó anteriormente, si un bloque sufre alguna alteración, su hash va a cambiar y se creará una discrepancia con las copias de las cadenas que tienen los demás participantes.

Transacciones:

La parte central de un bloque es la información de las transacciones que este posee, pero ¿qué es una transacción? Puede ser una línea de texto, un hash de un documento almacenado en otro lugar. Cada transacción es enviada a la red a través de un nodo y se combina con otras transacciones para generar un bloque. Es necesario que un bloque tenga varias transacciones, ya que, si se agrega cada transacción de manera individual se genera la posibilidad de una colisión. En el caso de que dos usuarios de la red agreguen el mismo registro en posiciones diferentes y más o menos al mismo tiempo, crearía una discrepancia con el número del registro, para evitar esto, se crea un bloque consolidado con varias transacciones.

Nonce:

Este es un número aleatorio que se utiliza en la minería de prueba de trabajo para intentar encontrar un hash que sea válido, es de un sólo uso y el objetivo de este es garantizar la integridad y la seguridad en la red. Se utiliza concretamente como un protocolo de autenticación.

Encabezado:

En el encabezado de un bloque se pueden encontrar los metadatos de este; contiene información clave como el hash del bloque anterior, la versión del software, la marca de tiempo, el nonce, la dificultad del objetivo (la dificultad del cálculo de la prueba de trabajo) y el Merkle Tree Root (es una estructura de datos que representa la relación entre las transacciones de un bloque).

Marca de tiempo:

Representa el tiempo en segundos de creación del bloque. Esta información va en el encabezado del bloque y sirve para confirmar que la fecha coincida en caso de un intento de alteración, con esto se prueba la integridad y la propiedad ante cualquier documento o contrato en la blockchain.

Hash del bloque:

Cada bloque debe tener un identificador único para que pueda ser hallado de manera inequívoca, en blockchain se usa el algoritmo SHA-256, ya que es conocido por su seguridad y eficiencia, este algoritmo produce un hash de 256 bits para cada bloque. En este algoritmo, sin importar cuál sea la entrada, el resultado siempre va a tener una longitud fija, además, cualquier cambio o alteración que se produzca en el bloque, va a generar un hash completamente diferente, lo que permite encontrar discrepancias de manera rápida y sencilla entre los usuarios de la red.

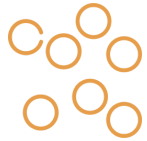
Número del bloque:

Es el identificador de la posición del bloque en la cadena, incrementa 1 con cada bloque que se haya añadido.

Cadenas de bloques

Ahora se conoce la arquitectura y elementos que contiene cada bloque, cuáles son sus principales funciones y cómo ayudan a la red a identificar la integridad en los datos. Ahora, se van a describir algunos conceptos más amplios que aparecen en el blockchain para que este pueda funcionar.

Consenso



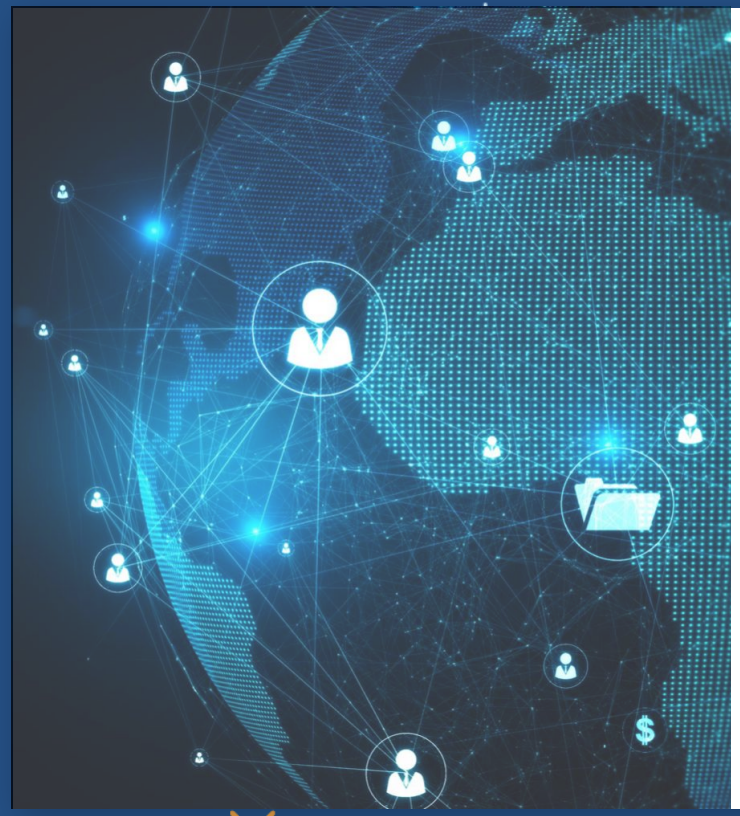
Descentralización

Criptografía

Consenso:

En blockchain se emplea un algoritmo de consenso llamado "Prueba de Trabajo" (PoW), es un desafío matemático para validar bloques. Una vez resuelto, el bloque se agrega a la cadena, y el nodo que resuelve el desafío recibe una recompensa en el sistema que se esté minando, por ejemplo, si se está minando en Bitcoin, la recompensa por la operación va a ser en bitcoins.

En lugar de PoW, algunas redes blockchain pueden optar por otros algoritmos de consenso, como la "Prueba de Participación" (PoS). Este cambio se hizo evidente debido a preocupaciones sobre el consumo de energía y la eficiencia de PoW. Ethereum, la segunda cadena de bloques más grande después de Bitcoin, realizó la transición de PoW a PoS en septiembre de 2022 mediante un evento llamado "La Fusión". En PoS, los participantes reciben recompensas según la cantidad de criptomoneda que poseen y utilizan para respaldar la red, en lugar de depender de la potencia computacional como en PoW. Este cambio contribuye a una mayor eficiencia energética y reduce la necesidad de realizar cálculos intensivos en miles de máquinas.



Descentralización:

La descentralización funciona a través del libro mayor distribuido, el cual permite a los usuarios tener independencia de cualquier autoridad o sistema central que tenga poder de alterar la red a conveniencia. Los usuarios tienen la posibilidad de hacer transacciones económicas o de información sin necesidad de tener un intermediario. Con el sistema descentralizado, se hace improbable que alguien pueda alterar los registros, ya que para realizar esta acción debería tener el 51% de los nodos de la red, lo cual es demasiado difícil en redes grandes por la cantidad de usuarios y capacidad de cómputo global.

Criptografía:

En blockchain se utilizan algoritmos criptográficos con el objetivo de asegurar la integridad de los datos y la autenticidad de estos. Como se mencionó en la estructura de los bloques, estos están enlazados a través de un hash, generando una cadena inmutable. También, se usan firmas digitales, las cuales sirven para garantizar la autenticidad del bloque en la cadena.

COLOMBIA POTENCIA DE LA VIDA

TIC

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira