

BOOTCAMP BLOCKCHAIN

INTEGRADOR - Módulo 1
UNIDAD 2



Complejidad Algorítmica y Sistemas pares de Claves Públicas y Privadas

En una blockchain es necesario garantizar la seguridad y la integridad de los datos y registros que se agregan con cada nuevo bloque. Tener en cuenta la eficiencia de los algoritmos aplicados en los diferentes procesos puede ayudar a tomar decisiones importantes sobre la estructura del sistema implementado.

- Los algoritmos de hashing son la mejor manera de mantener la integridad en los datos de los bloques en una blockchain. Comprender los conceptos básicos de los algoritmos y poder categorizar su eficiencia con una notación estandarizada es una buena forma de entender a profundidad cómo se conecta cada parte de una blockchain, por qué es necesario tener una complejidad algorítmica en los mínimos niveles posibles.

Contextualización de los Aprendizajes

Este módulo está diseñado para una semana estructurada de la siguiente manera

En la primera lección se explicarán los conceptos asociados a la representación de algoritmos y su complejidad con la notación Big O.

En la segunda lección se va a profundizar los algoritmos de hashing y cuáles son algunos de los más relevantes en las tecnologías actuales.

En la tercera lección se van a usar los conocimientos aprendidos hasta el momento para explicar qué son los sistemas pares de claves públicas y privadas, y cuál es su importancia para mantener la seguridad en una blockchain.



Objetivo general

UNIDADES 2

Al finalizar esta unidad el estudiante estará en capacidad de:

- Representar visualmente un algoritmo con diagramas de flujo.
- Analizar la complejidad algorítmica usando notación Big O.
- Analizar los algoritmos de hashing más usados y su importancia en el blockchain.
- Identificar las principales características de los sistemas pares de claves públicas y privadas.

Competencias a desarrollar

- Capacidad de abstracción, análisis y síntesis.
- Capacidad para representar un algoritmo.
- Compresión de la complejidad algorítmica.
- Comprensión de los sistemas pares de claves públicas y privadas.

Capacidad de abstracción análisis y síntesis: Reconocer y entender los conceptos mostrados en la unidad.

Capacidad para representar un algoritmo: Entender cómo hacer la representación visual de un algoritmo con diagramas de flujo.

Comprensión de la complejidad algorítmica: El estudiante reconoce la eficiencia de un algoritmo dado y la clasifica con notación Big O.

Comprensión de los sistemas pares de claves públicas y privadas: El estudiante lee y comprende textos relacionados con cifrados simétricos y asimétricos.

CONCEPTOS BÁSICOS

Tiempo de ejecución: 10 horas

PLANTEAMIENTO DE LA SESIÓN

Se sugiere repartir el contenido de la presente unidad en tres (3) sesiones de dos (2) horas cada una o dos (2) sesiones de tres (3) horas cada una. La metodología sugerida para las sesiones es de Aula Invertida, en la que, se dejan como tarea antes de la sesión lecturas al estudiante. Se inicia la sesión con una práctica y se acompaña al estudiante para que construya el desarrollo teórico luego de haber realizado la práctica. Esto con el fin de que el conocimiento adquirido sea deductivo a partir de la experiencia de las actividades.

Como actividad previa se debe preguntar a los estudiantes, qué entienden ellos por el concepto de algoritmo, complejidad algorítmica, algoritmos de hashing, y sistemas pares de claves públicas y privadas en criptografía.

MATERIALES

- Computador con conexión a internet.



COLOMBIA
POTENCIA DE LA
VIDA



TIC

**TALENTO
TEC**

AZ | **PROYECTOS
EDUCATIVOS**

UTP
Universidad Tecnológica
de Pereira