COLOMBIA POTENCIA DE LA VIDA

TIC

Conceptos **básicos para blockchain**

Lección 1

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Tiempo de ejecución: 6 horas

PLANTEAMIENTO DE LA SESIÓN	Materiales
En esta lección los estudiantes deberán poner a prueba sus conocimientos previos sobre los algoritmos, datos y la criptografía, para este fin deberán exponer lo que creen que significan estos conceptos y cuáles son sus principales características. + info	Calculadora de hash

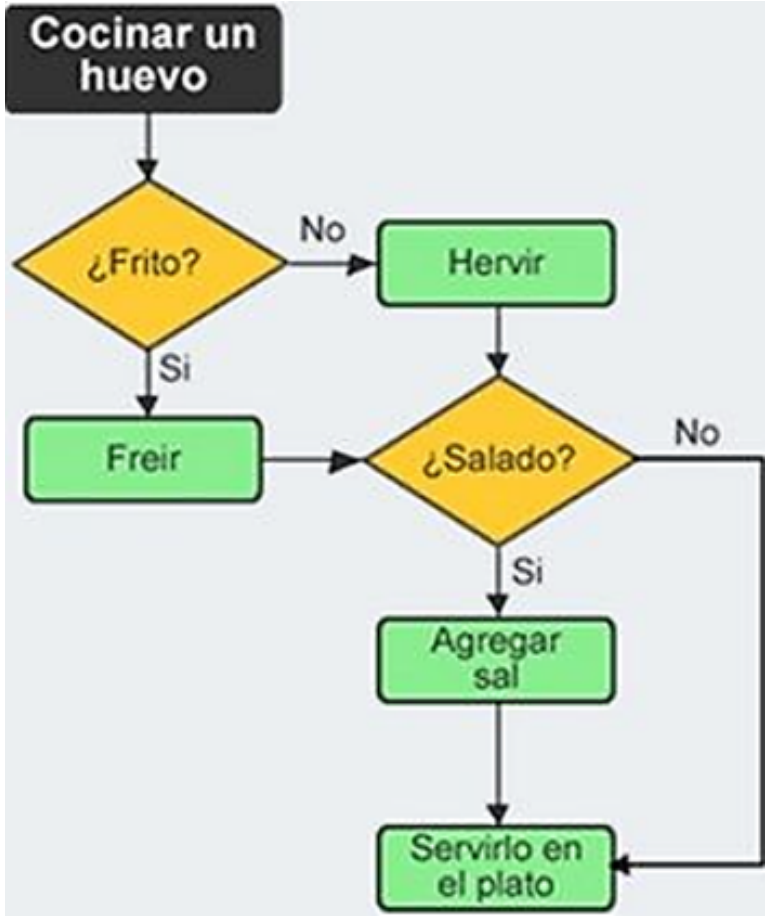
Desarrollo teórico de la sesión: 4 horas

Es necesario que investiguen a cerca de los diferentes tipos de datos que puede recibir un sistema y como ejercicio previo antes de la sesión, proponga los estudiantes hacer un algoritmo sobre una actividad cualquiera que realicen diariamente y también deben dar un ejemplo de una serie de pasos que no sea un algoritmo. Esto con el fin de poner en contexto a todos los estudiantes en estructuras algorítmicas.

Algoritmia

Un algoritmo es definido como un conjunto de instrucciones definidas, no ambiguas, ordenadas y finitas de un sistema o proceso para realizar una actividad concreta, por ejemplo, calcular el resultado de una ecuación matemática, procesar y transformar datos, preparar una receta de comida, etc. Hay algoritmos que pueden contener bucles de acciones en algunos de sus pasos, pero estos bucles deben tener un final establecido, en caso de que dicho bucle no tenga final, se puede decir que entonces no estamos hablando de un algoritmo, ya que es un proceso sin un final determinado.

Ahora vamos a ver el ejemplo de un algoritmo :



En este caso se puede notar que se cumplen con las cualidades de un algoritmo, sus instrucciones están bien definidas, no son ambiguas, están ordenadas y el algoritmo tiene un fin, servir el huevo en un plato. Si no se cumple alguna de las cualidades nombradas anteriormente, no estaríamos hablando de un algoritmo.

Para ejemplificar lo que no es un algoritmo, vamos a imaginar que nos reuniremos con una persona y le tenemos que dar indicaciones para llegar al lugar pactado, para esto le daremos el siguiente conjunto de instrucciones ordenadas:

- Debes ir al centro de la ciudad.
- Camina 3 cuadras hacia la derecha en la tienda de la esquina.
- Sube al quinto piso de un edificio que hay a mitad de cuadra.
- Puedes sentarte en la silla del pasillo para esperar a la hora de la reunión.

En el caso anterior tenemos una serie de instrucciones ordenadas, con un final, pero hay ambigüedad. ¿Cuál ciudad?, ¿la tienda de cuál esquina?, ¿en cuál cuadra está el edificio?, ¿a qué hora es la reunión?

En conclusión, aunque sean instrucciones ordenadas, incumplen con las cualidades de un algoritmo.

COLOMBIA POTENCIA DE LA VIDA

TIC

Datos

Un dato es el elemento central de los sistemas de información, normalmente son variables cuantitativas o cualitativas que describen un sistema y nos permiten su análisis posterior. La información entonces es un conjunto de datos procesados y organizados según los requerimientos del propio sistema.

+ info

Podemos obtener datos de todas partes y responder a preguntas de interés, por ejemplo, ¿cuántas personas hay en Colombia?, ¿cuántas personas hay en situación de desempleo? Con esta información procesada podemos plantear soluciones a problemas que se presentan en la sociedad y en el entorno.

Algunos tipos de datos son los números enteros, números con decimales, caracteres individuales, cadenas de caracteres o texto, valores booleanos de verdadero o falso, fechas y horas, y estructuras de datos complejas como matrices o tablas.

Estos tipos de datos deben ser procesados y categorizados correctamente, por ejemplo, si quiero crear la categoría “Números de teléfono” para un sistema de registro de llamada, los valores deben ser numéricos.

Por ejemplo, no sería corrector decir que el número de un cliente es “12/23/2023”. Al diseñar cualquier sistema que maneja información se deben tener en cuenta los tipos de datos que va a recibir el mismo para poder hacer un procesamiento correcto.

Los datos son de vital importancia en el blockchain, por este motivo debemos comprender bien los tipos de datos con los que nos podemos llegar a encontrar para poder categorizarlos, procesarlos, transformarlos y analizarlos. Veamos algunos ejemplos con dos conjuntos de datos.

- **Conjunto A:** {rojo, carro, manzana, pelota, computador, casa}
- **Conjunto B:** {nombre, edad, nacionalidad, nivel académico}

Los elementos del conjunto A claramente son datos, pero ¿podemos hacer algo con ellos? Parecen ser datos aleatorios y no los podríamos categorizar para hacer un análisis sobre lo que nos quiere decir el conjunto. Ahora, ¿qué hay del conjunto B? Podemos ver datos cualitativos que podríamos categorizar, procesar y analizar para realizar diversos estudios, tomando una muestra de personas y preguntando por esas cualidades podemos obtener un conjunto de datos que nos sería útil para responder algunas posibles preguntas sobre una población determinada.

Criptografía

La criptografía es el estudio y práctica de técnicas para proteger la información a través de diversos mecanismos como los algoritmos codificados, hashes y firmas. La información que queremos proteger con la criptografía puede estar en un archivo, un documento de texto, puede estar en tránsito a través de la comunicación de dos aplicaciones o podría estar en uso. Los principales objetivos de la criptografía son la confidencialidad de la información, la integridad de los datos (que no se hayan manipulado o alterado), autenticar la identidad de un usuario o la autenticidad de un documento, y evitar que un usuario deniegue actividades anteriores.

Los orígenes de la criptografía tienen que ver con los mensajes y el envío de información sensible, un mensaje que podría parecer completamente aleatorio puede contener información importante sobre actividades o códigos para realizar alguna acción.

En este contexto, una carta con un mensaje puede encriptarse para que parezca algo aleatorio o común para una persona que no sea el destinatario de dicha carta, por ejemplo, al enviar una carta a un amigo deseando bienestar para él y su familia se puede crear un mensaje con información sensible que solo el remitente podría descifrar, para cualquier otra persona parecería una carta de saludo formal común y corriente.

Algoritmo de hashing

Son funciones con diferentes algoritmos matemáticos que transforman una entrada o información en una salida o cadena de longitud fija, la cual identificamos como “hash”. Entre las cualidades de la función hash están la longitud fija, lo cual hace referencia a que la longitud del hash es independiente del mensaje de entrada, siempre va a conservar su longitud. Es determinista e irreversible, si le damos el mismo mensaje de entrada a la función siempre nos va a devolver el mismo hash, pero no podemos hacer un proceso inverso en el cual sepamos lo que dice un mensaje original únicamente usando el hash resultante. Resistente a colisiones, al usar diferentes mensajes o entradas sería demasiado difícil obtener un mismo hash resultante. Por último, un pequeño cambio en la entrada podría resultar en un hash completamente diferente. Ahora vamos a ver algunos ejemplos de la función hash, hay diversas funciones para obtener un hash, pero nos vamos a enfocar en la función SHA-256 (Secure Hash Algorithm 256-bit), ya que es la función criptográfica por excelencia en el mundo del blockchain.

Calculadora de hash

Tomemos la entrada “Hola mundo” con algunas variaciones y usemos la función SHA-256 para ver el hash resultante, en el siguiente link se puede acceder a una calculadora de hash:

Ver tabla

Entrada (mensaje)	Salida (hash)
Hola mundo	ca8f60b2cc7f05837d98b208b57fb6481553fc5f1219d59618fd025002a66f5c
hola mundo	6f2a99cda22eeb252d0d1ac5c0bf6d43f33344f9442c66548abc1d3207533bf1
hola Mundo	00256edc2cabb60f547b376373e936ac4a5ba78a0ca00960eea3703ac2a707c5
HOLA MUNDO	fe66f29e4ae43f0bde571567bdca37c9360f14481739c01269f11923f54f5575
Hola mundo	ca8f60b2cc7f05837d98b208b57fb6481553fc5f1219d59618fd025002a66f5c

Como podemos ver en la tabla anterior, al cambiar solamente una letra de minúscula a mayúscula obtenemos un hash completamente distinto al de la cadena original “Hola mundo”, y si al final volvemos a poner la cadena original, nos retorna el mismo hash de la primera vez en todas las ocasiones.