

## Módulo 1

# LECCIÓN 3

## Taller de cadenas de bloques y consenso pdf



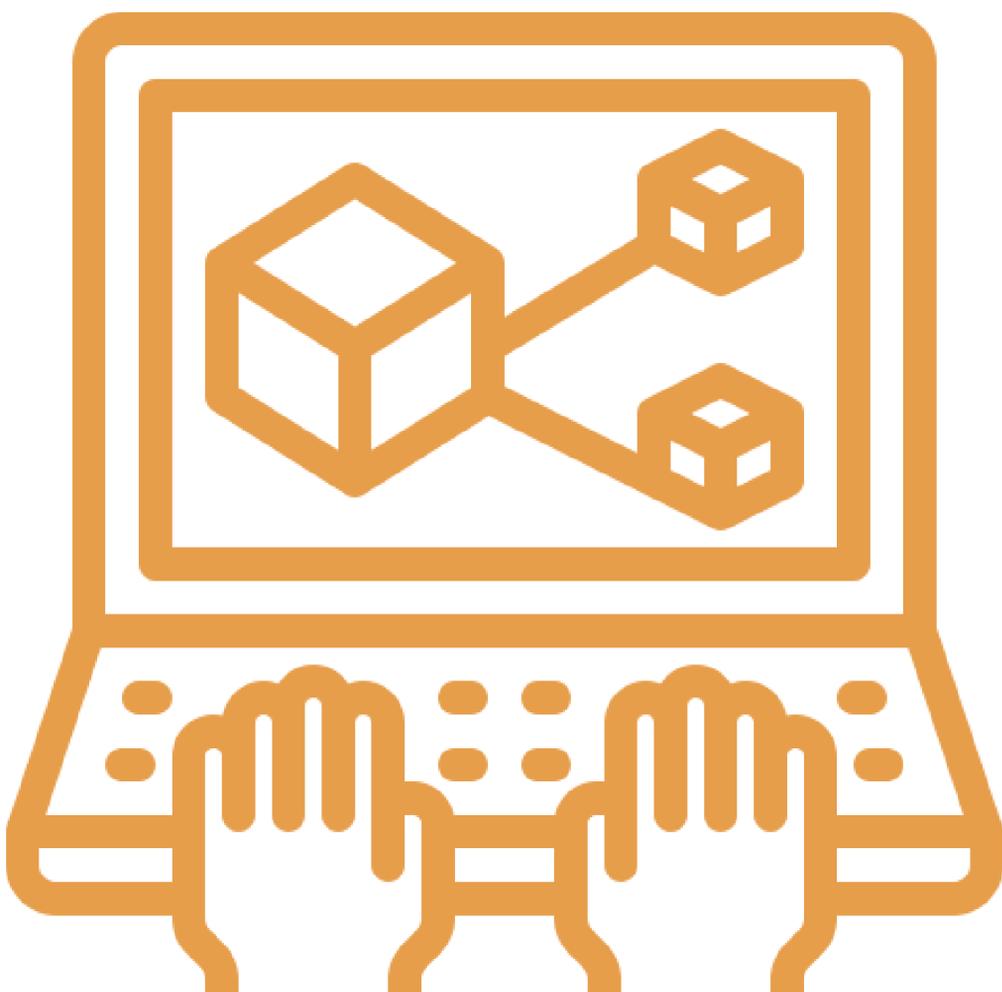
Se propone que los estudiantes creen su propia blockchain manualmente. El grupo completo debe participar para crear la red.

## Indicaciones:

- Cada integrante del grupo tiene 10,000 unidades con las cuales pueden hacer transacciones entre ellos, por ejemplo, comprar objetos ficticios o información. Ejemplo de transacción: "Transferir 1,000 unidades a Estudiante B".
- Debe haber un libro público en el que se registren todas las transacciones realizadas por los miembros del grupo, cada integrante debe tener un número de identificación y un alias, los cuales van a aparecer cada que hagan una transacción con otro integrante.
- Cada vez que se realiza una transacción, la mayoría debe estar de acuerdo con el nuevo registro (al menos el 51%). Antes de realizar el registro, cada integrante tiene que revisar el libro público para verificar que existen las unidades suficientes para realizar dicha transacción, en caso de una discrepancia, la transacción debe ser anulada.
- Cada registro de transacciones debe ir en un bloque de información, que contenga los principales elementos de la estructura que se vio en la lección 1 (encabezado con los datos del tiempo, el hash del bloque anterior, el hash del bloque actual, el número del bloque y la transacción realizada). Los estudiantes se deben reunir en pequeños grupos para decidir las transacciones que van a ir dentro del bloque.
- Cada grupo presenta su bloque al resto de la clase, explicando las transacciones incluidas. El resto de la clase (nodos) verifica la validez de las transacciones y aprueba o rechaza el bloque mediante consenso. Si la mayoría aprueba, el bloque se agrega a la cadena; de lo contrario, se requiere consenso para realizar cambios o correcciones.

- Para ingresar un nuevo bloque en la cadena, se debe introducir alguna entrada en la calculadora de funciones hashing y obtener el valor del SHA-256, el cual debe quedar registrado en el libro público para asociarlo a cada bloque.
- Cada integrante puede intentar alterar el bloque que se va a registrar, por ejemplo, pagando en una transacción con más unidades de las que realmente tiene o alterando la cadena existente modificando registros y hashes. El objetivo es que todos estén atentos para que esto no suceda.
- Si un estudiante detecta una transacción no válida en un bloque o un registro existente que ha sido alterado, puede advertirlo. Los estudiantes deben argumentar a favor o en contra de la validez de las transacciones.
- Cuando uno de los participantes es descubierto intentando alterar los registros, los demás participantes pueden decidir si sacarlo de la red o no, se debe hacer una votación y la decisión se toma con el 51% de votos a favor.
- El juego termina cuando el tiempo se acaba o la mayoría del grupo haya sido sacado de la red.

Al finalizar la actividad, se propone hacer una reflexión grupal sobre los desafíos y aprendizajes. Se pregunta a los estudiantes sobre la importancia del consenso y la seguridad en una cadena de bloques.



## LISTA DE CHEQUEO DE LO QUE APRENDÍ

Carácter de los desempeños	Indicador por evaluar	Si	Parcialmente	No
<ul style="list-style-type: none"> <li>Dar cuenta de cómo funciona la arquitectura de una cadena de bloques y cuáles son los elementos principales de cada uno.</li> </ul>	Comprendí cuáles son los elementos de un bloque y sus principales funciones.			
	Comprendí cómo funciona el consenso y la descentralización en una blockchain.			
	Entendí cuál es la importancia de las pruebas de trabajo al agregar un bloque nuevo en una blockchain.			
<ul style="list-style-type: none"> <li>Comprender el funcionamiento de la función SHA-256 y su importancia en la seguridad de una blockchain.</li> </ul>	Reconocí los pasos iniciales para calcular el hash de un mensaje usando la función SHA-256.			
	Comprendí el motivo para utilizar una función de hash en una cadena de bloques para validar la integridad y seguridad de los registros.			