

L U M B R E



Blockchain y Bitcoin: cómo ponerse de acuerdo en quién tiene la razón sin nadie que mande

Materia: Tecnología

04/10/2026

Antes de empezar

El video de Memorias de Tiburón es el detonador. Alrededor entendemos el registro distribuido, la minería, las claves públicas y los límites reales de la tecnología.

QUÉ APRENDERÁS

- Entender el problema de doble gasto que resolvió Bitcoin, cómo funciona una cadena de bloques y por qué la confianza descentralizada cuesta energía y no es perfecta.

El problema de confiar sin jefe

Durante siglos, llevar un registro en el que todos estuvieran de acuerdo exigió un árbitro: un banco, un notario, un gobierno. Su trabajo era decir quién tiene razón cuando dos personas reclaman lo mismo. En 2008 un documento firmado por un tal Satoshi Nakamoto mostró otra salida: hacer que miles de computadoras independientes mantengan el mismo libro contable y se vigilen entre sí, sin dueño. Bitcoin nació ahí. La pregunta de fondo no es si el bitcoin sube o baja: es si una red puede generar confianza sin nadie a quien reclamarle. Piensa: ¿qué pasaría con tu dinero si desapareciera hoy el banco que lo registra?

Antes de ver



Bitcoin. Imagen: Satheesh Sankaran (CC BY-SA 2.0), Wikimedia Commons.

- El "doble gasto" es el problema: impedir que el mismo dinero digital se gaste dos veces.
- Un blockchain es un libro de cuentas copiado en miles de nodos que se sincronizan.

- Los bloques se encadenan con funciones hash: alterar un dato viejo invalida todo lo posterior.
- La minería compite por resolver un acertijo criptográfico y así elige el siguiente bloque.

Mientras ves el video, ten presente esta pregunta: si nadie manda, ¿qué impide que la red mienta?

El video

VIDEO

¿Qué es Bitcoin y cómo funciona?

Canal: Memorias de Tiburón. Explicación sencilla sin humo financiero.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=rryQmSdWW6g>

Mientras lo ves

1. Identifica qué papel juega la clave pública y cuál la privada.
2. Busca por qué minar consume tanta electricidad.
3. Anota qué diferencia hay entre el dinero de un banco y uno descentralizado.

Lo importante

La invención clave no fue un dinero nuevo sino un método de consenso. Cada nodo guarda una copia del historial completo; cuando alguien quiere transferir, firma la orden con su clave privada y la difunde. Los mineros agrupan transacciones en un bloque y compiten encontrando un número que, al pasar por la función hash, dé un resultado por debajo de cierto umbral —un acertijo que no se puede resolver con inteligencia, solo con intentos—. El primero en hallarlo lo anuncia, todos lo validan y lo añaden. Como cada bloque incluye el hash del anterior, alterar una transacción vieja exigiría recalcular toda la cadena y superar al resto de la red: barato de verificar, carísimo de falsificar.

De ahí salen las promesas y también los costos. Ventajas: cualquiera con internet puede participar sin permiso, el historial es auditable y la emisión es predecible —habrá 21 millones de bitcoins, ni uno más—. Desventajas: el diseño convierte la

electricidad en seguridad —cada bloque nuevo es trabajo computacional despilfarrado a propósito para hacer caro mentir—, el anonimato es relativo (las direcciones son pseudónimos y el rastro es público), y la inmutabilidad significa que no hay "des-hacer": una clave perdida es un dinero muerto para siempre, y una estafa queda escrita en piedra. Blockchain no es confianza mágica: es confianza cara de producir.

Algo que el video no te contó

El día que Bitcoin pagó una pizza

El 22 de mayo de 2010, un programador de Florida llamado Laszlo Hanyecz publicó: "Le doy 10 mil bitcoins a quien me traiga dos pizzas del tamaño grande". Se las llevaron, y la transacción quedó en el bloque de por vida. Hoy esas pizzas valdrían cientos de millones de dólares. El episodio, celebrado cada año como Bitcoin Pizza Day, es a la vez el mejor ejemplo del problema que resolvió Bitcoin —dos desconocidos se pusieron de acuerdo sin árbitro— y el mejor chiste sobre su volatilidad.

Tu turno: razona el costo

1. ¿Por qué la minería consume tanta electricidad si "solo" lleva una contabilidad?

- ☐ Porque los servidores están muy fríos
- ☐ Porque la seguridad se compra con trabajo: hacer caro el intento de falsificar es lo que vuelve creíble el registro
- ☐ Porque bitcoin necesita climatizar el dinero
- ☐ Porque las transacciones son archivos enormes

Comprueba si lo entendiste

2. ¿Qué problema resolvió el diseño de Nakamoto?

- ☐ La lentitud de los bancos
- ☐ El doble gasto sin necesidad de un árbitro central
- ☐ La volatilidad del precio
- ☐ La falta de cajeros automáticos

3. Las bitcoins pueden emitirse sin límite según decida la red.

- ☐ Verdadero
- ☐ Falso

4. ¿Por qué alterar un dato antiguo de la cadena es casi imposible?

- ☐ Porque hay una copia en un banco central
- ☐ Porque cada bloque incluye el hash del anterior: cambiar el pasado obliga a recalcular todo lo demás
- ☐ Porque los mineros lo impiden votando
- ☐ Porque el software lo bloquea

5. Un registro sin dueño resuelve desconfianzas pero desperdicia energía y no tiene a quién reclamarle un error. ¿En qué trámite de tu país confiar en un árbitro es peor que confiar en una red? ¿Y al revés?

Piensa en escrituras, actas de nacimiento o resultados electorales.

Sigue explorando

Fuentes

Blockchain — Wikipedia <https://es.wikipedia.org/wiki/BlockchainArquitectura>, consenso y variantes.

Memorias de Tiburón <https://www.youtube.com/@MemoriasdeTiburonCanal> divulgador del video detonador.

Referencia curricular

Materia:	Tecnología
-----------------	------------

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://lumbre.lat/object/explora-blockchain-y-bitcoin>

Material educativo generado desde Lumbre · lumbre.lat