

eurecat

"innovating for business"

**"Què pot aportar la tecnologia
Blockchain en el món dels residus?"**



Juan Caubet, PhD
Director of IT&OT Security Unit
juan.caubet@eurecat.org
@juancaubet

www.eurecat.org

eurecat

"innovating for business"

¿Qué es la tecnología Blockchain?

¿Qué es la tecnología Blockchain?

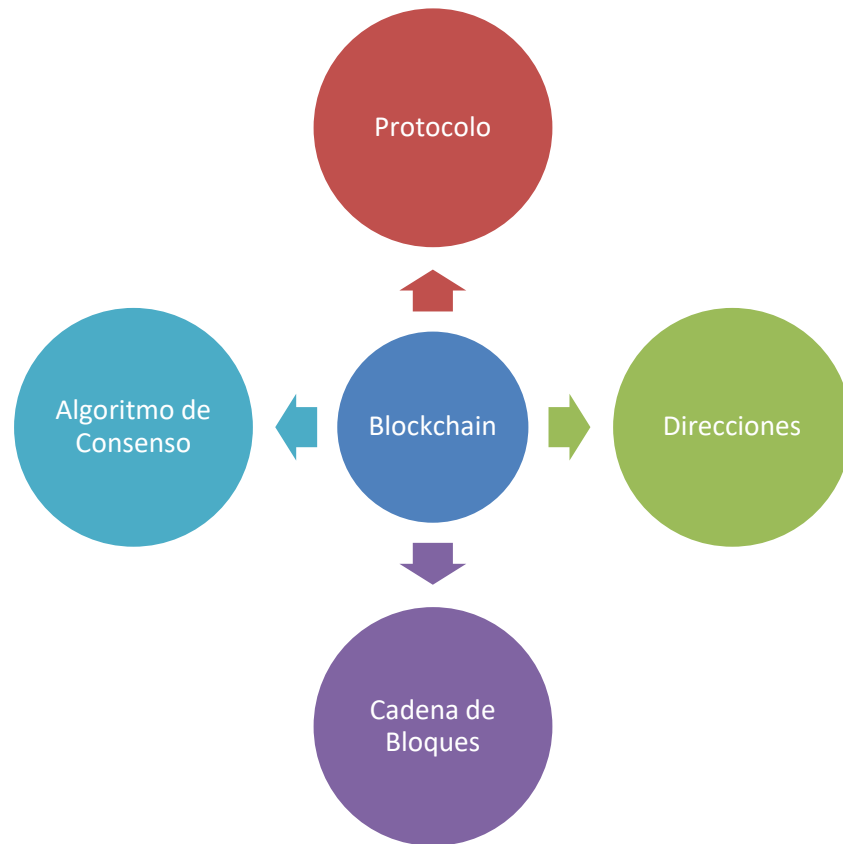
Tecnología Blockchain **≠** Criptomonedas

La tecnología Blockchain permite a entidades sin confianza llegar a un consenso sobre un histórico digital compartido.

¿Qué es la tecnología Blockchain?

Una Blockchain es un **Registro de Transacciones** y eventos digitales, cuya información es aprobada por **Consenso** y... almacenada en **Bloques** de transacciones **Enlazados** criptográficamente, de forma **Descentralizada** (red P2P distribuida).

Características de las Blockchain



- **Descentralización**
- **Inmutabilidad**
- **Transparencia/Trazabilidad**
- **Escalabilidad**
- **Eficiencia**

Tipos de Blockchain

Públicas (permissionless)

No existe una autoridad gobernante.

- Cualquiera puede acceder al sistema, leer datos, registrar transacciones y/o crear bloques.



Privadas/Híbridas (permissioned)

El sistema está gestionado por un grupo de organizaciones.

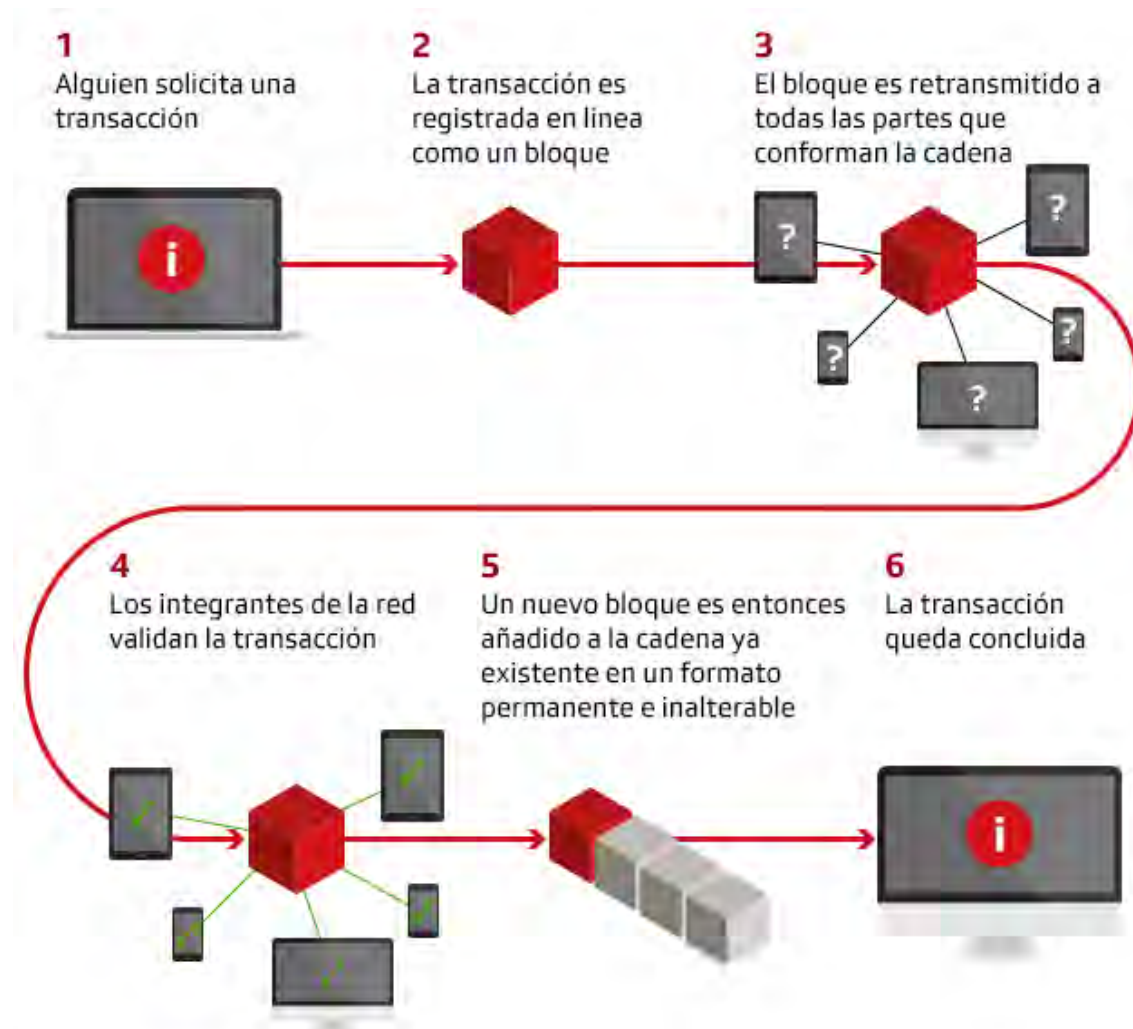
- Se pueden necesitar permisos para acceder al sistema, leer datos, registrar transacciones y/o crear bloques.



HYPERLEDGER PROJECT



¿Cómo funcionan?



Fuente: Financial Times, PwC Estados Unidos

El Algoritmos de Consenso

- **Problema de los Generales Bizantinos**

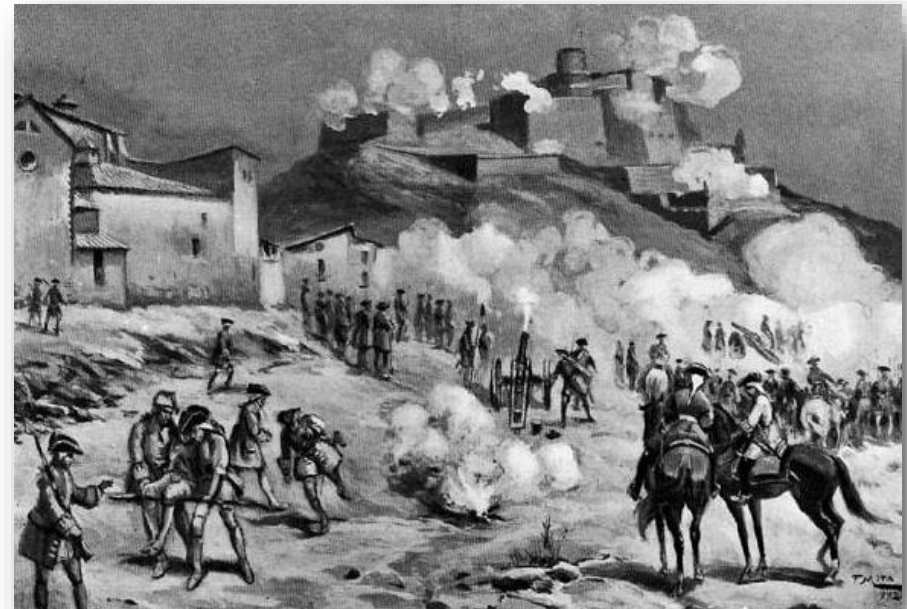
Una ciudad está siendo asediada por un ejército, donde cada división es comandada por un general.

El asedio sólo tendrá éxito si todos los generales atacan al mismo tiempo.

Las comunicaciones entre divisiones se realizan utilizando mensajeros.

Algunos mensajeros y generales son traidores.

- ¿Cómo conseguimos que todos los generales leales tomen la misma decisión?



Tipos de Algoritmos de Consenso

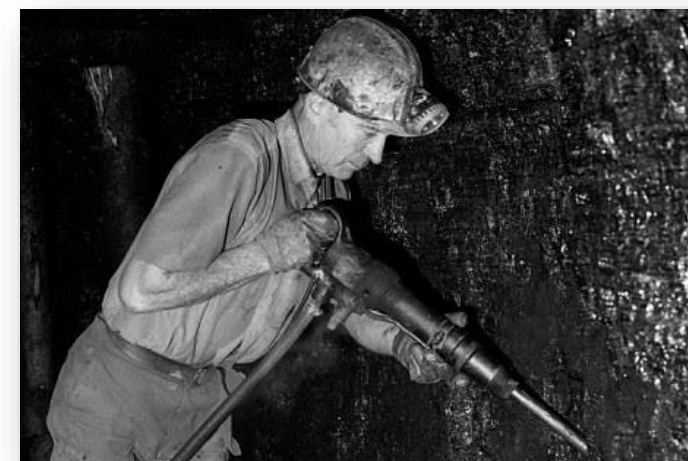
- **Proof of Work (PoW)**

IDEA: Resolver un problema matemático complejo.

El nodo dispuesto a crear un bloque debe realizar una serie de *Blockhashes*.

PROS: El minero se compromete con el sistema porque obtiene una recompensa.

CONS: Consume una gran cantidad de energía.



Fuente: <http://i.dailymail.co.uk>

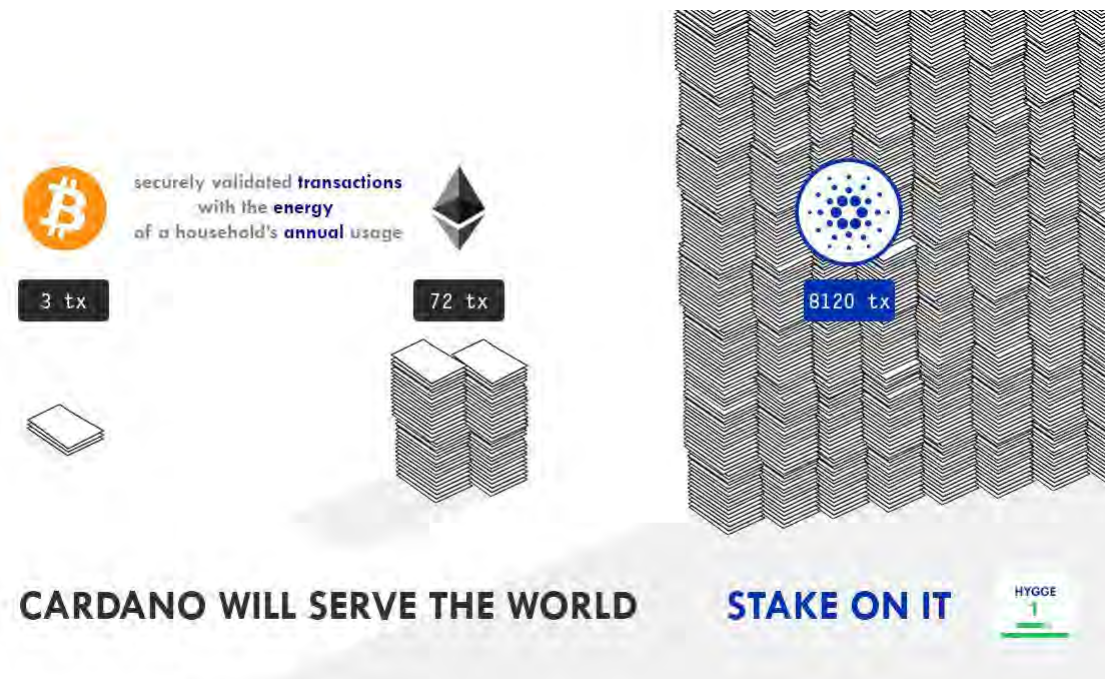
Consumo de energía

LA RAZÓN

Medio ambiente

Cómo reducir la voracidad eléctrica de las criptomonedas

A día de hoy hay más de 8.000 criptodivisas en circulación. En unos 10 años el valor de este nuevo mercado ha crecido hasta los 1.000 millones de dólares. La divisa reina, Bitcoin, supone el mismo gasto energético que un país como Chile, porque su seguridad se basa en ~~“minar” o resolver complejos algoritmos~~ criptográficos. Sin embargo, mucha de la competencia de Bitcoin está cambiando sus sistemas de seguridad por alternativas que eviten esos costosos cálculos matemáticos



'Ethereum 2.0' PoS Blockchain Aims to Cut Energy Use by 99%

Tipos de Algoritmos de Consenso

- **Proof of Stake (PoS)**

IDEA: Cuantos más tokens tenga un nodo, más posibilidades tendrá de crear un bloque.

Una vez que se elige un nodo, el resto de nodos no necesitan realizar cálculos.

PROS: Consume mucha menos energía que la PoW.

CONS: Incrementa las diferencias entre nodos ricos y nodos pobres.



Fuente: <https://medium.com>

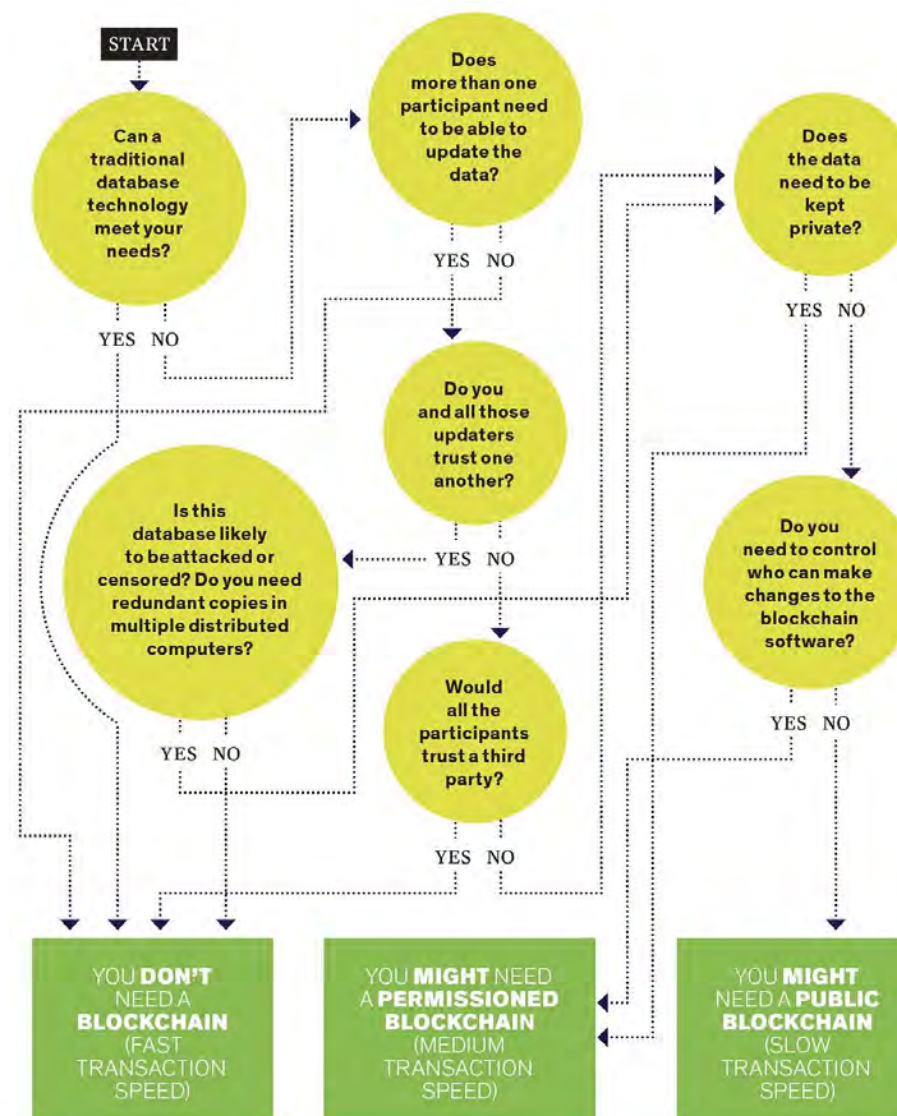
Smart Contracts

- Los Smart Contracts son trozos de **código**.
 - Una vez en la Blockchain son **inmutables**.
 - Todos los nodos ejecutan el mismo código.
- Dotan de “**inteligencia**” a la Blockchain.
 - Permiten **automatizar procesos**.

Tokenización de Activos

- Tokenizar es **representar un derecho en una Blockchain**, concretándose dicha representación en anotaciones contables unitarias llamadas **tokens**.
- Esos tokens van ligados a una cuenta concreta (*wallet*) y **pueden ser transferidos**.
- La **naturaleza jurídica** de lo que queremos tokenizar determinará cuál es su régimen de propiedad, de transmisibilidad o de responsabilidad.
- El token sirve como **prueba de titularidad** de un derecho y puede considerarse como un **instrumento financiero** (*security token*).

¿Cuándo tiene sentido utilizar una Blockchain?



eurecat

"innovating for business"

Aplicaciones de la Tecnología Blockchain

Supply Chain - Trazabilidad



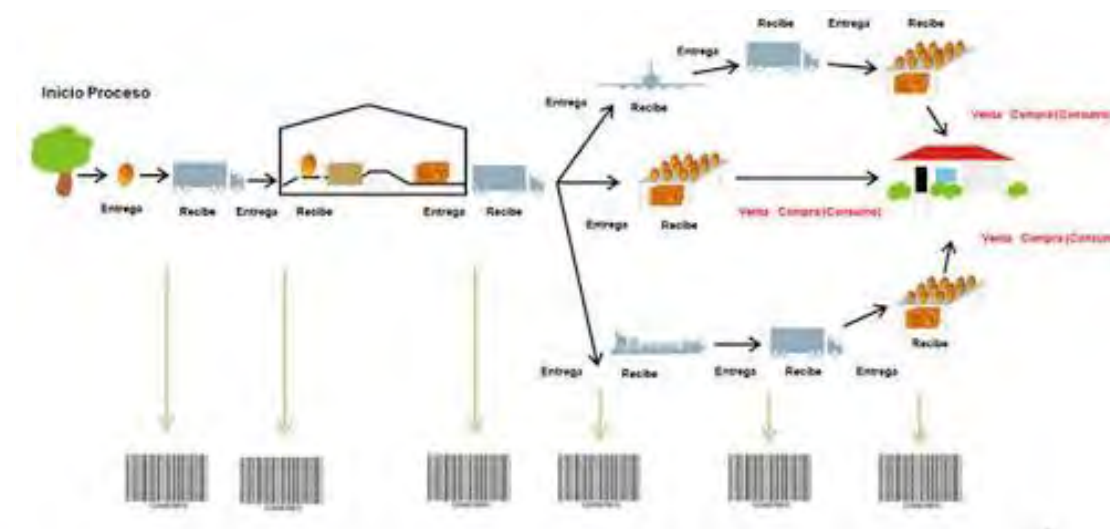
- ✓ Proporciona una plataforma donde los diferentes actores pueden compartir información.
- ✓ Consolida y asegura los datos, y los hace disponibles a quien corresponda.

- Busca proporcionar transparencia y confianza.
- Ecosistema formado por puertos, operadores marítimos, transportistas terrestres, autoridades aduaneras, etc.



Supply Chain - Trazabilidad

- ✓ Proyecto de trazabilidad de plantas ornamentales para una cooperativa de productores.
- ✓ El objetivo es registrar las diferentes etapas de crecimiento de las planta, así como sus certificados ecológicos.
- ✓ Este nuevo sistema también ayudará a mejorar los controles de stock y suministros.
- ✓ El comprador final podrá escanear un código QR y ver todos los datos asociados a la planta.



Traçabilitat i Gestió de Residus

Traçabilitat i circularitat dels aparells elèctrics i electrònics i els seus residus.

- ✓ Sistema que permeti traçar i localitzar els AEE comercialitzats a Catalunya des del mateix moment de la seva fabricació.
- ✓ Traçar **l'estat** i ubicació dels aparells quan esdevenen residus, RAEE.
- ✓ Proporcionar informació dels components que contenen els AEE i es defineixin com estratègics.
- ✓ Crear una cadena de confiança per tal de que els recursos econòmics que els fabricants **d'AEE** han **d'aportar** per a la correcta gestió dels RAEE es distribueixin **d'una** forma segura i honesta entre els diferents agents implicats.

USE CASE

Waste transport on Blockchain

How the Ministry of ILT saved EUR 7M by sharing data and business logic with competitors and governments.

<https://www.ltonetwork.com/use-cases/waste-transport-on-blockchain>

“Con LTO eliminamos gastos administrativos por gestionar los permisos y procesos relacionados con el transporte internacional de residuos. Los documentos en papel han dejado de existir. Las partes interesadas pueden validar y verificar el proceso y los datos por sí mismos, sin depender de nosotros.”

Gestió de Residus



Generalitat de Catalunya
Centre de Telecomunicacions
i Tecnologies de la Informació

- ✓ Sistema electrònic de registre dels Fulls de Seguiment (FS) de **l'Agència** de Residus de Catalunya (ARC) basat en tecnologia Blockchain.
- ✓ Diferents actors (operadors, productors, transportistes i gestors de residus) actuen com a signataris en les diferents fases del tràmit realitzat en **l'extranet** de **l'ARC** (SDR).
- ✓ Beneficis:
 - Alta disponibilitat, robustesa i fiabilitat.
 - Seguretat de la informació.
 - Traçabilitat de les actuacions.
 - Veracitat de la informació.
 - Accessibilitat i usabilitat.



¡Gracias!

Dr. Juan Caubet

juan.caubet@eurecat.org

Director de la Unidad de IT&OT Security