

La seguridad de blockchain como disrupción global para bitcoin y otras aplicaciones

Alejandro Hernandez

01/11/2018



- Es una divisa? Un bien de cambio? Un activo?
Una burbuja?
- Siempre se habla de expectativas.
Expectativas de qué?
- Dónde reside la confianza? (valor,
devaluación, etc.)



- Estamos ante un **cambio disruptivo**, y no es precisamente el bitcoin.
- Bitcoin es una **aplicación de** la tecnología **blockchain** (está implementado sobre esta).
- Blockchain es una tecnología que define, entre otras cosas:
 - Estructura de datos
 - Algoritmo de almacenamiento para los datos
 - Protocolo de comunicación
 - Protocolo de "consenso" (para determinar datos válidos e inválidos)



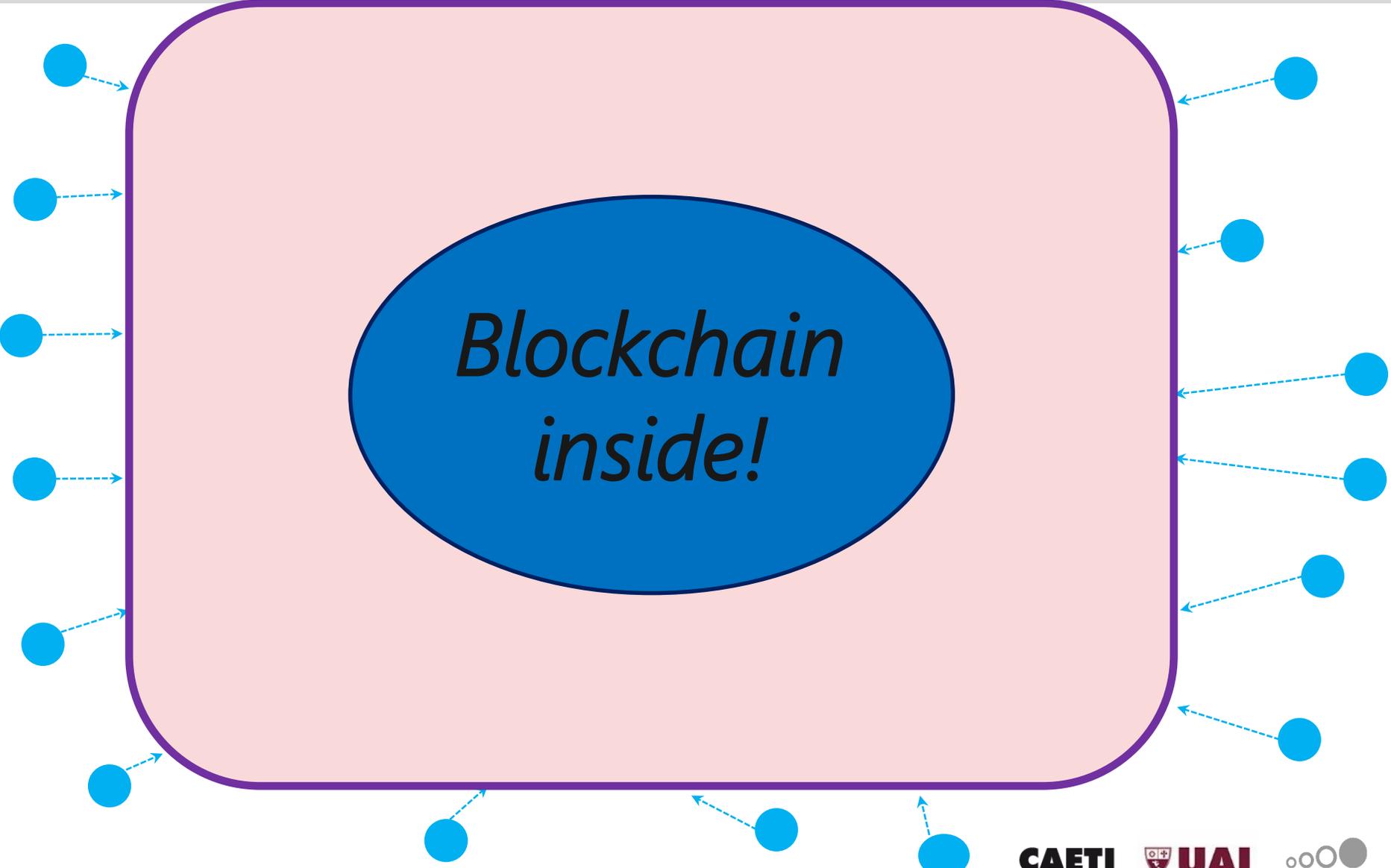
- *Qué es y cómo se usa blockchain*
- *Cómo funciona blockchain*
 - Transacciones
 - Red p2p
 - Protocolo de comunicación y consenso
- *El ecosistema actual*
 - Contratos inteligentes
 - Aplicaciones existentes, en desarrollo y futuras



Qué es y cómo se usa blockchain



Blockchain es UNA COMPUTADORA



Algunas condiciones para usar blockchain



- Muchos participantes comparten los datos ("ven" lo mismo)
- Muchos participantes cambian los datos (se tienen que guardar correctamente)
- Verificabilidad (participantes necesitan confiar con desconfianza)
- Eliminar intermediarios (costo, conciliaciones, etc.)
- Eliminar interacciones (tiempo)
- Interrelación entre transacciones (dependencia mutua o múltiple)



- **Descentralización** de confianza
- Realización de propiedades de **seguridad** (integridad y disponibilidad)
- Un **nuevo horizonte revolucionario** para la elaboración de un sinnúmero de ideas.

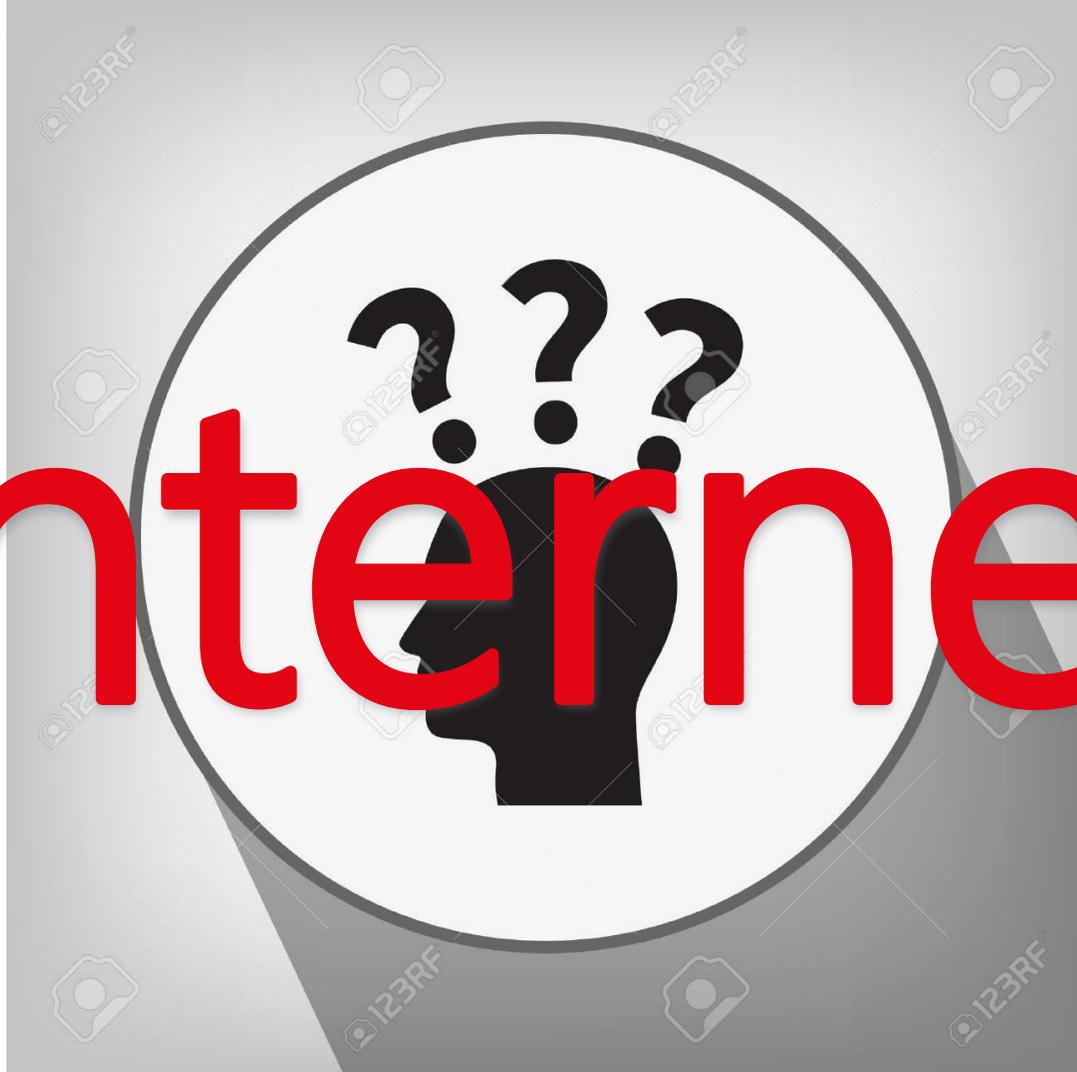
Cuál es LA tecnología disruptiva de nuestra era?



Cuál es **LA tecnología** disruptiva de nuestra era?



Internet



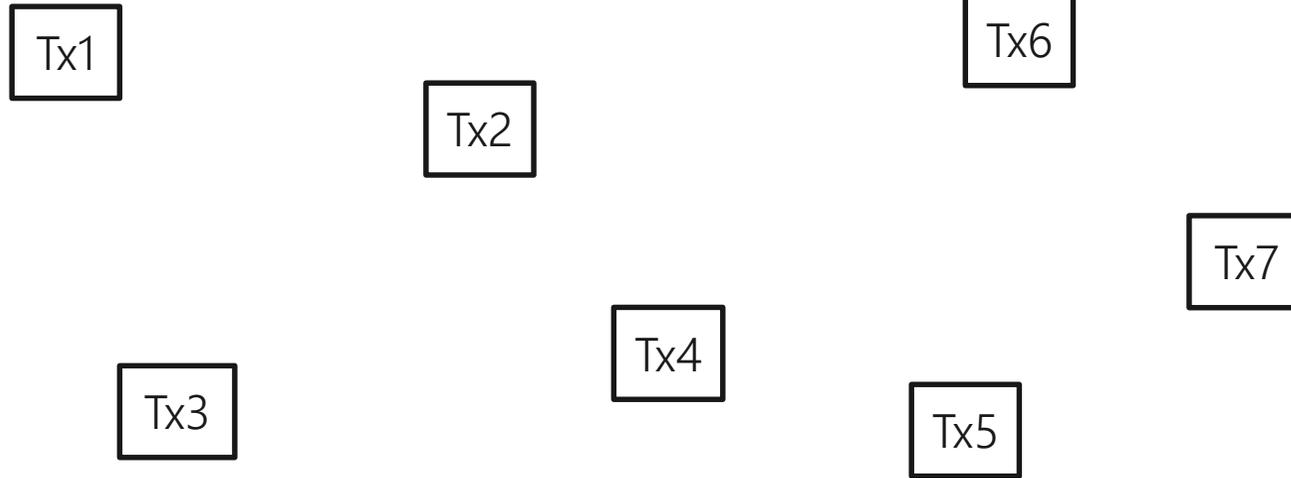


Cómo funciona blockchain

Transacciones

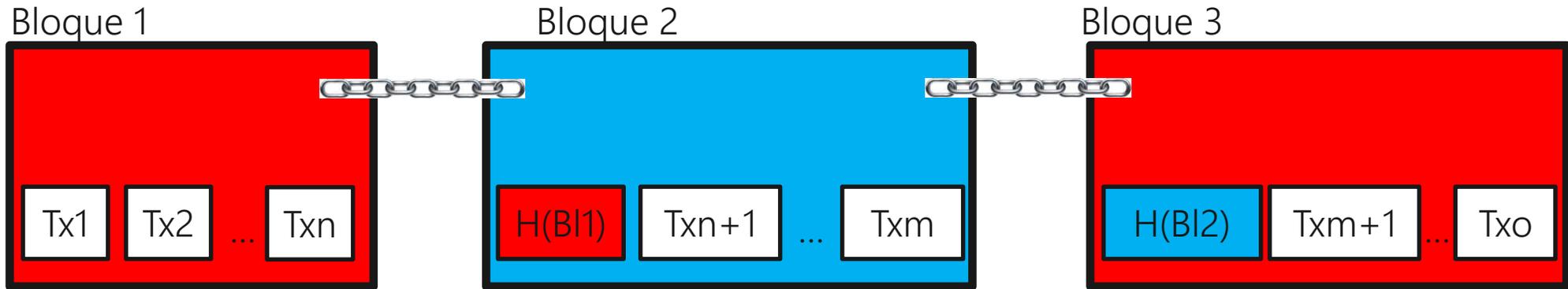


La cadena de bloques (transacciones individuales)



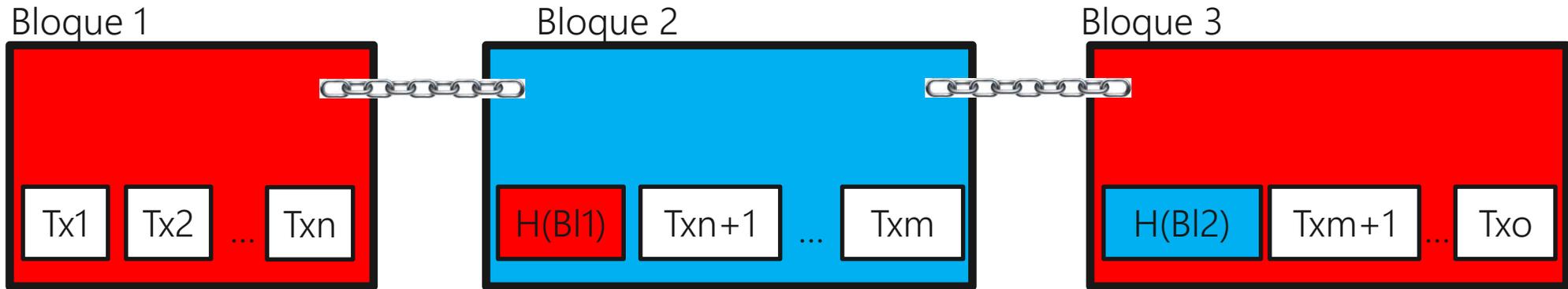
- **Transacción: cualquier dato** que merezca ser guardado (para reflejar un **evento, suceso** o **cambio**):
 - La información de que X le pasó dinero a Y
 - El nombre del nuevo dueño de una casa
 - La ejecución de un programa
 - Una foto de una luna de Júpiter
 - El nombre del autor de una canción o libro

La cadena de bloques (agrupando transacciones)

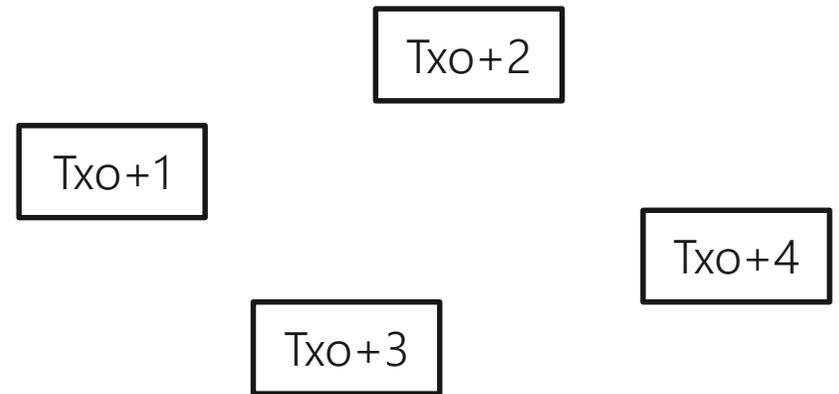


- Cada bloque tiene una “**huella**” del inmediato anterior
 - Esto impide que se modifique
 - Por inducción, ninguno de los bloques anteriores se modifica
- Esto se sostiene combinando fuertes mecanismos de seguridad (**hashing**, **encriptación** de clave asimétrica).

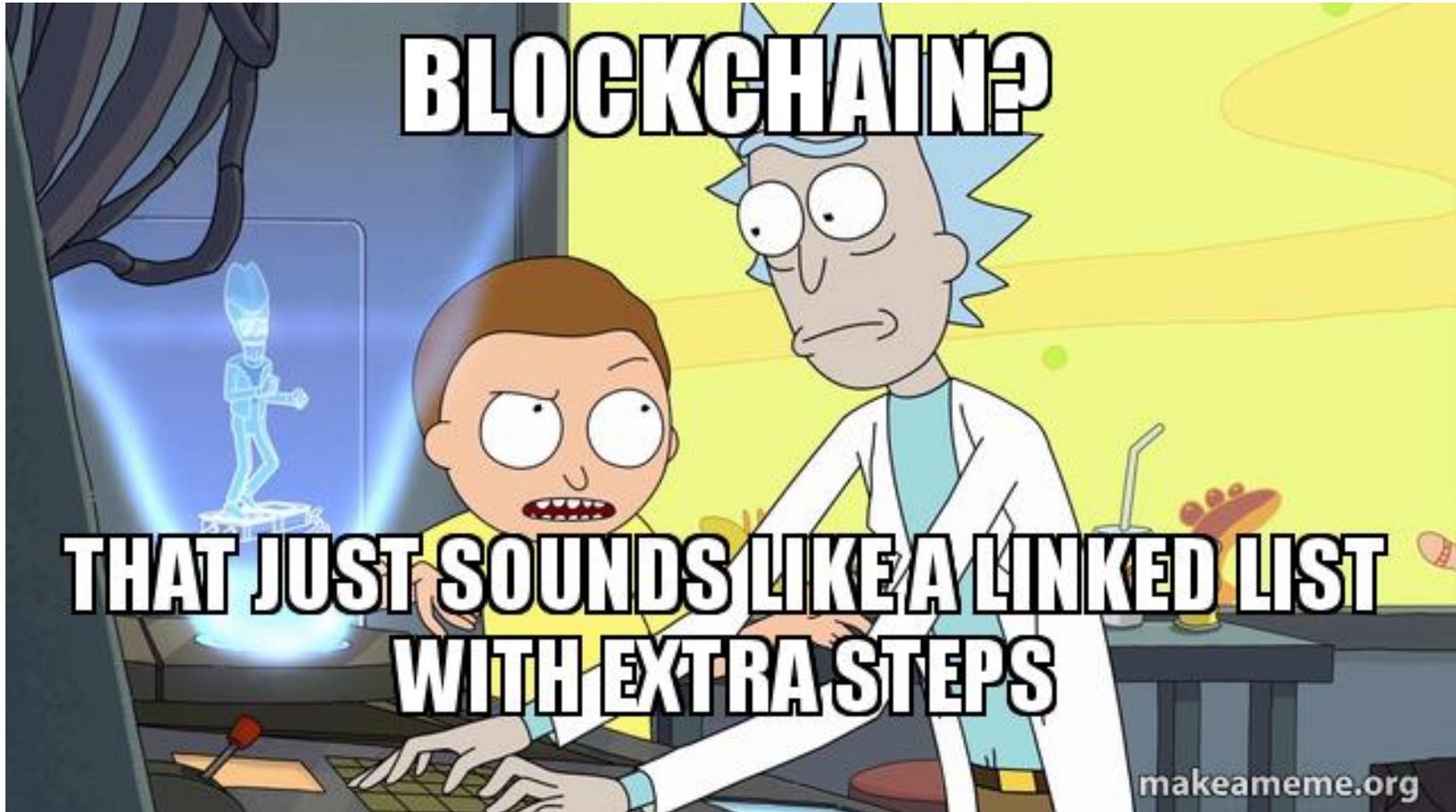
La cadena de bloques (nuevas transacciones)



- Cuando se cierra un nuevo bloque (y se "encadena" al anterior), todas estas nuevas transacciones quedan validadas.



Es "un poco" más que una estructura de datos



- Blockchain?
- Suena como si fuera un lista enlazada con algunos pasos adicionales

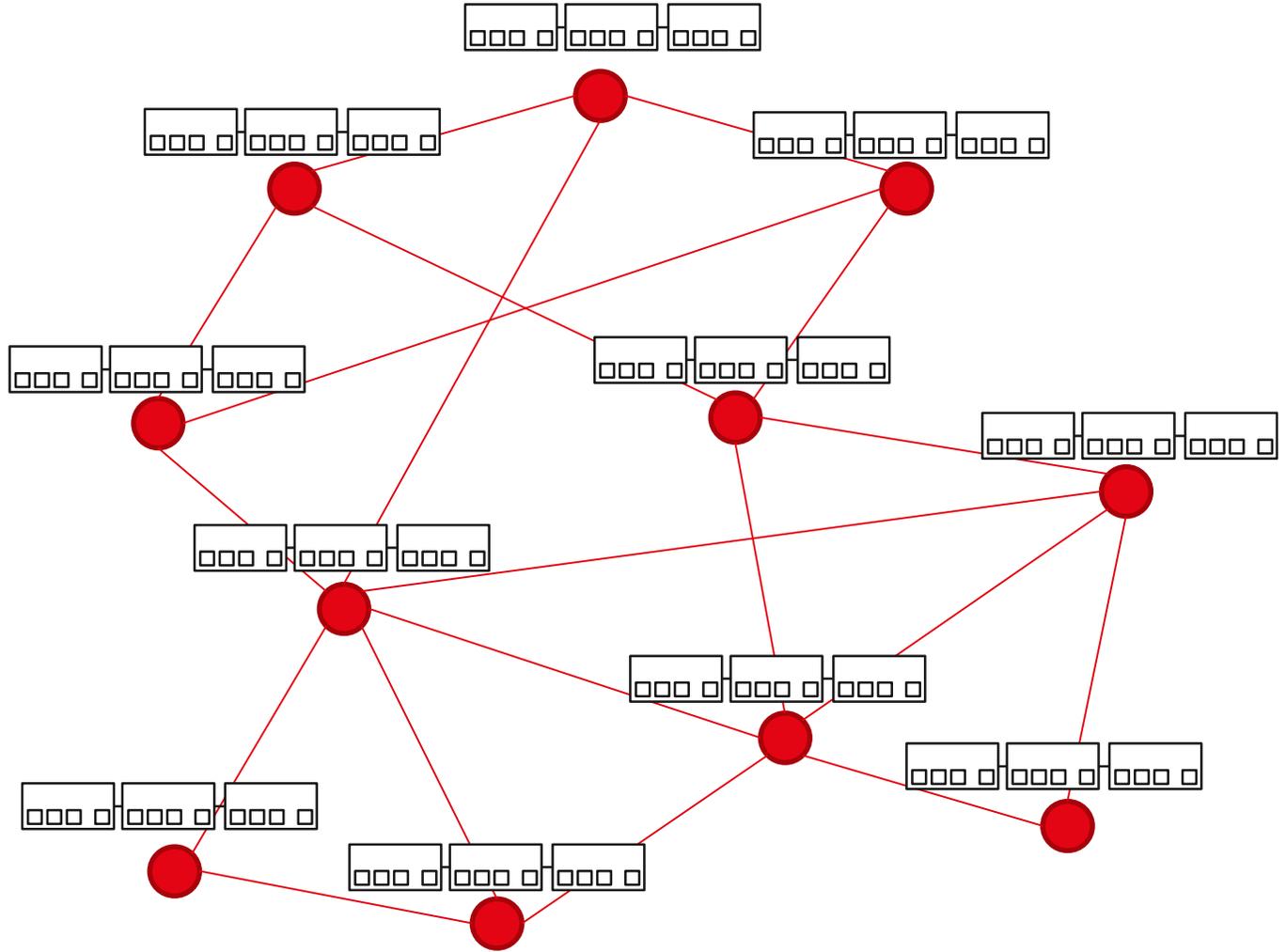


Cómo funciona blockchain

Red p2p



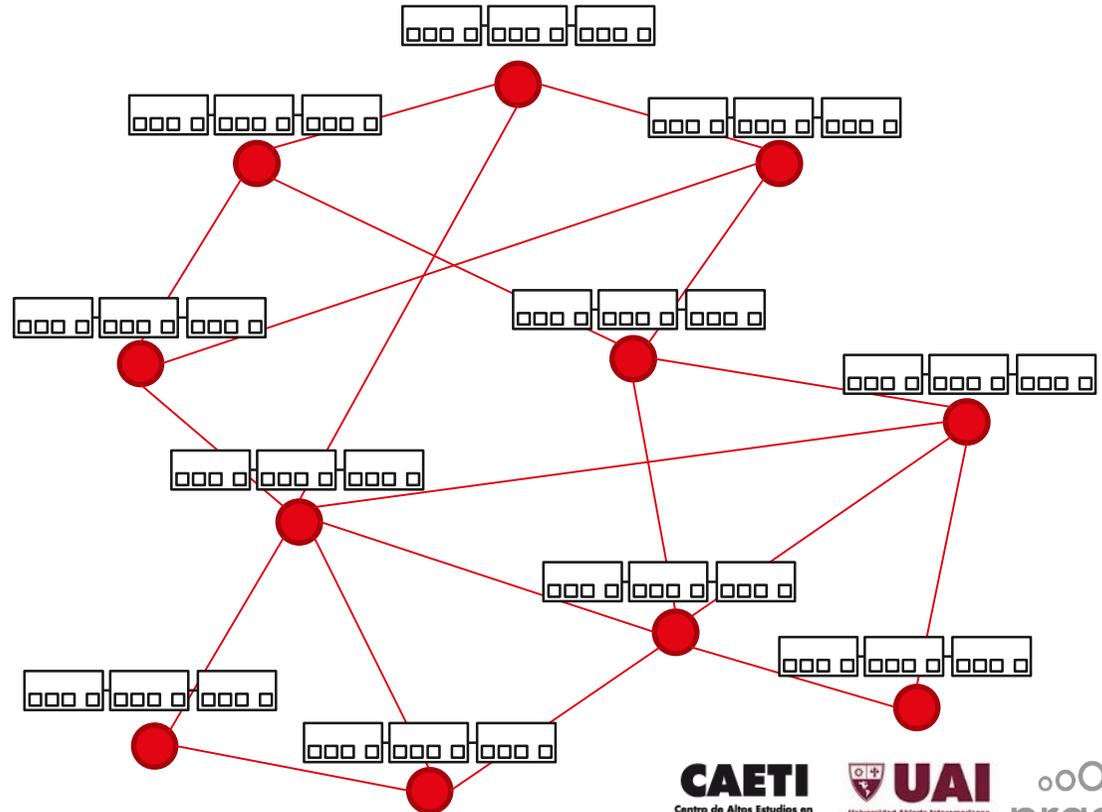
Red peer-to-peer (de nodos, o mineros)



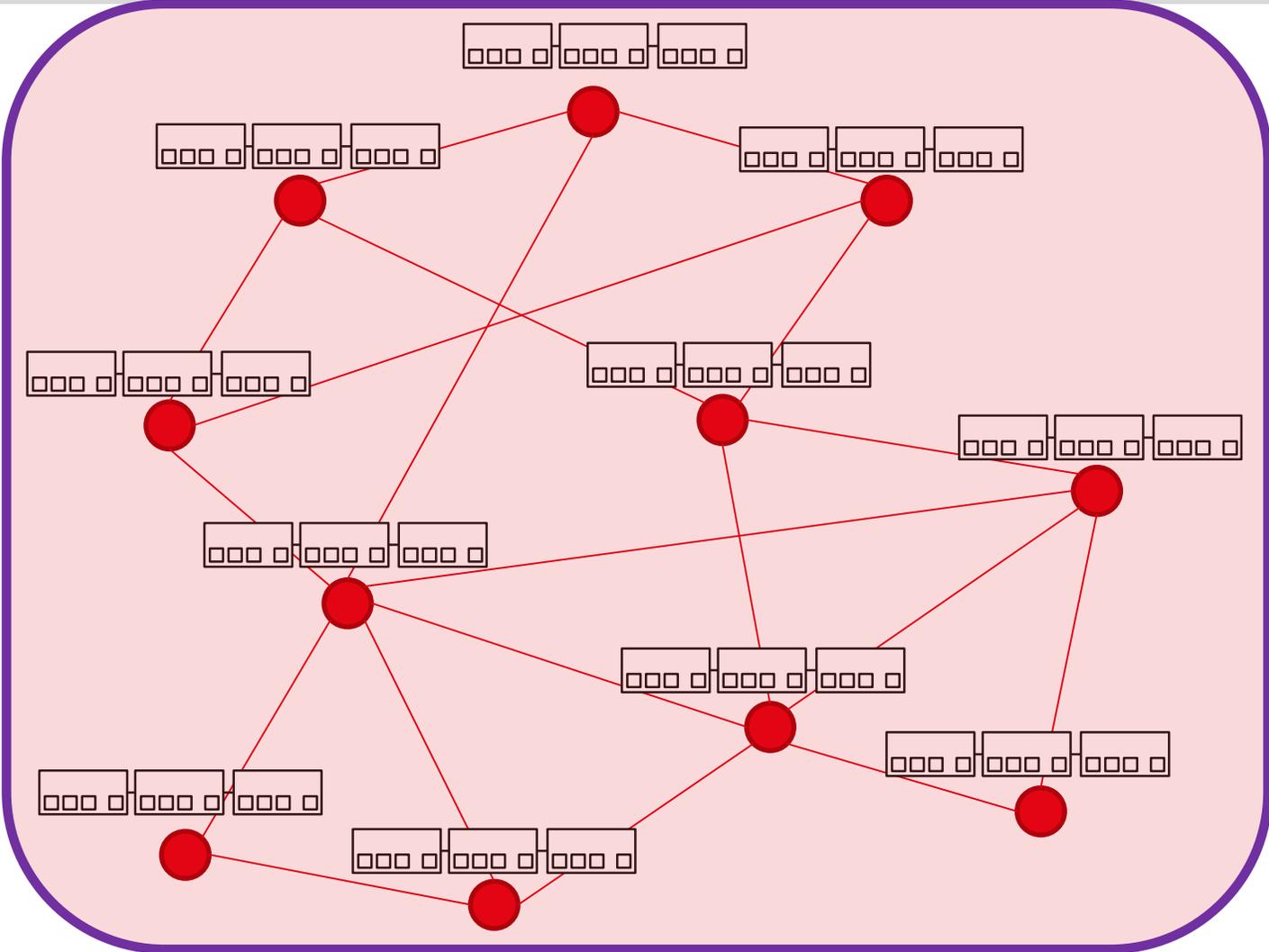
Características de la cadena de bloques



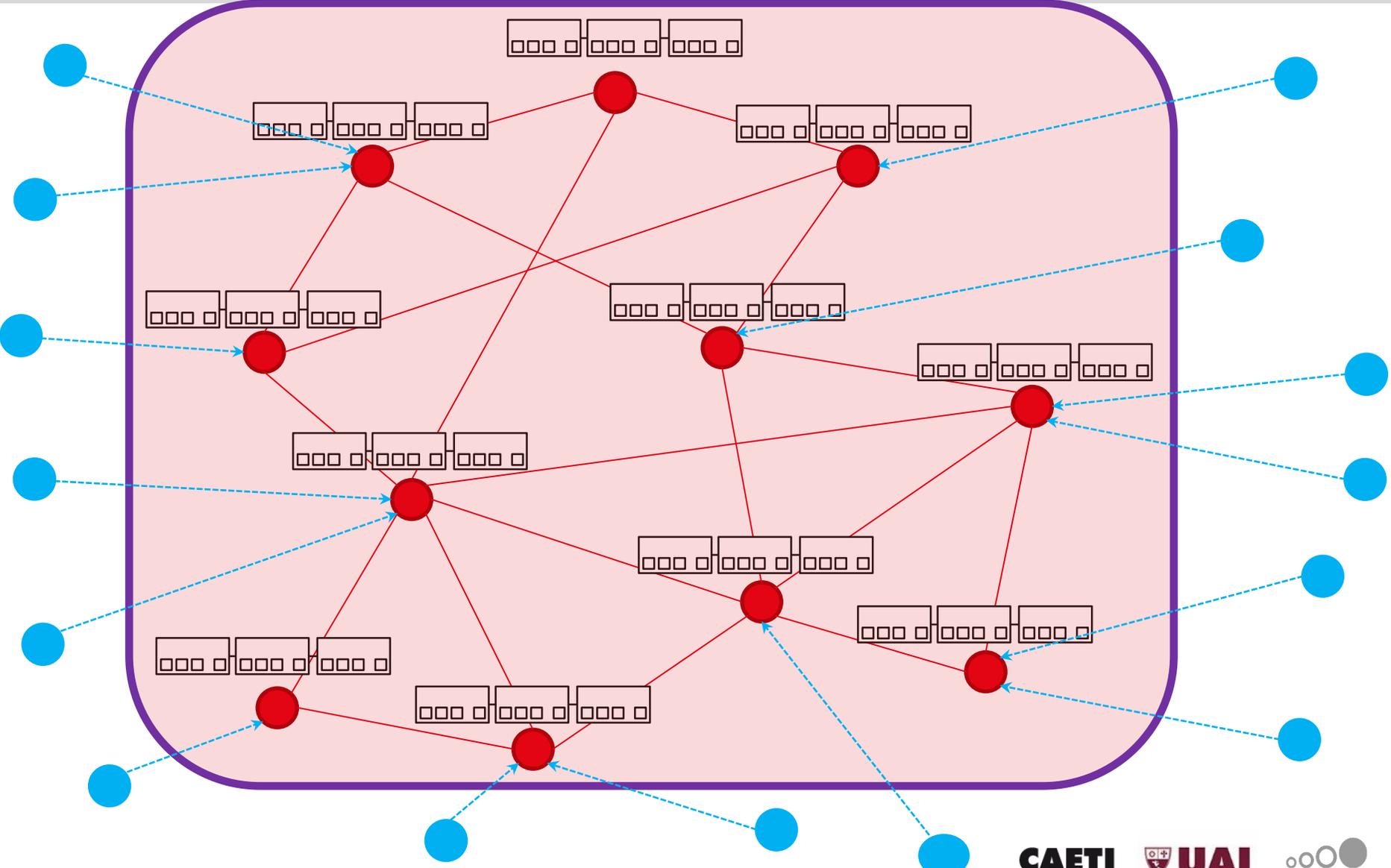
- Cadena está replicada en todos los nodos (verificable, auditable):
 - Esto elimina intermediarios / se basa en consenso distribuido.
 - **Disponibilidad** inmediata.
- Trazabilidad e inmutabilidad, de cualquier tipo de transacción.
 - Non-repudiation.
 - **Integridad** absoluta.



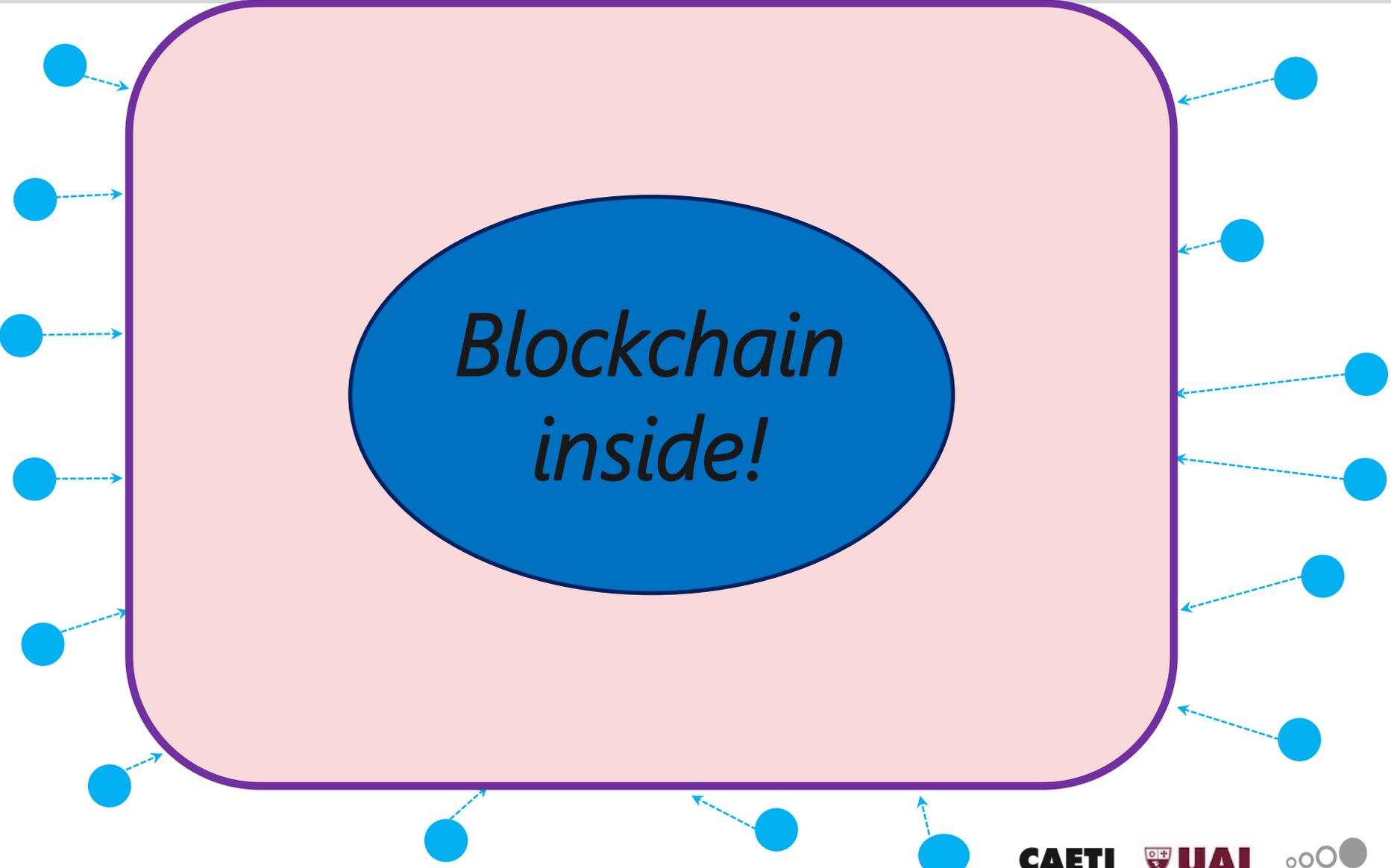
La computadora global (visión interna)



La computadora global (visión ampliada con usuarios)



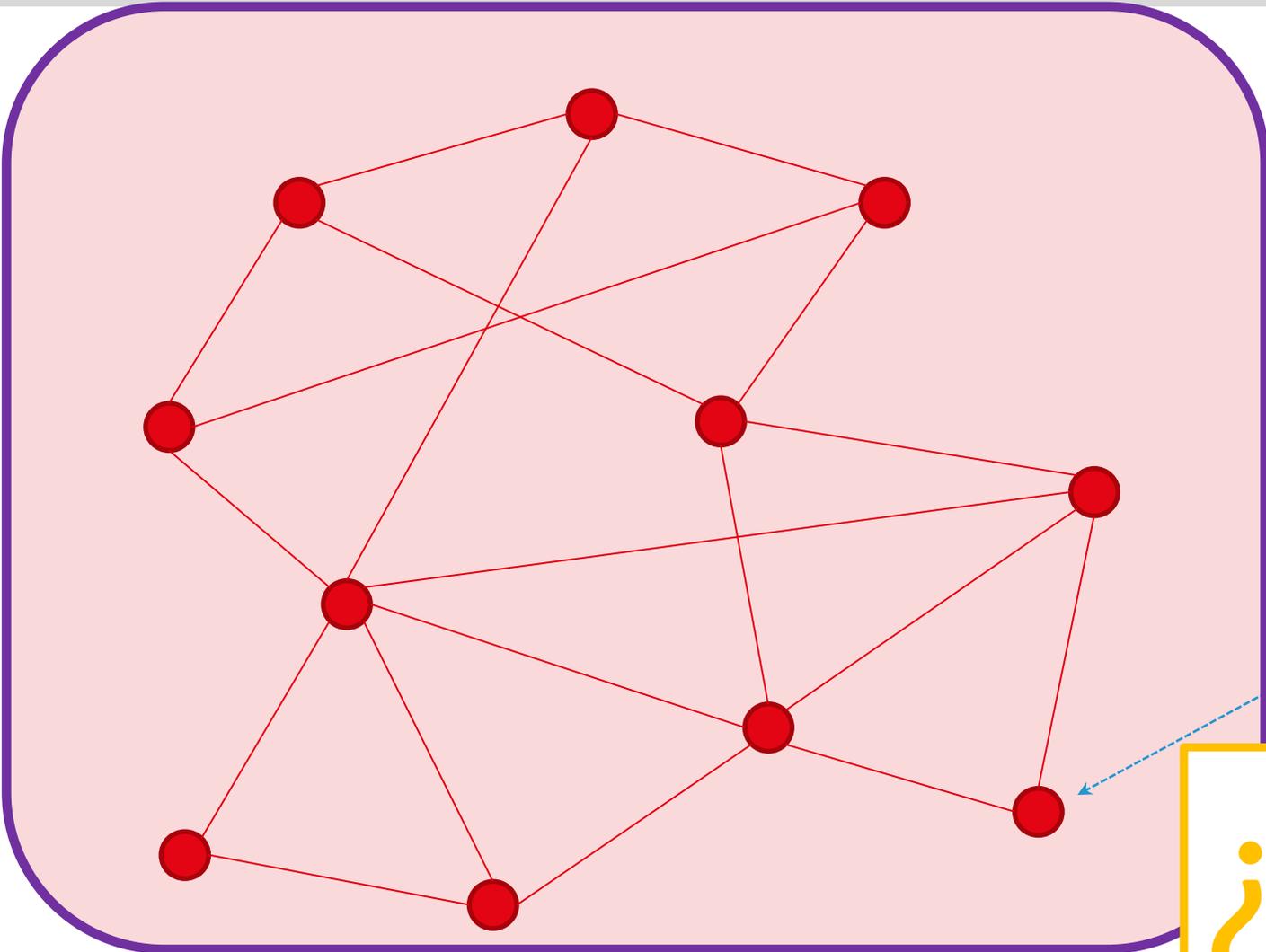
La computadora global (visión externa)



Cómo funciona blockchain

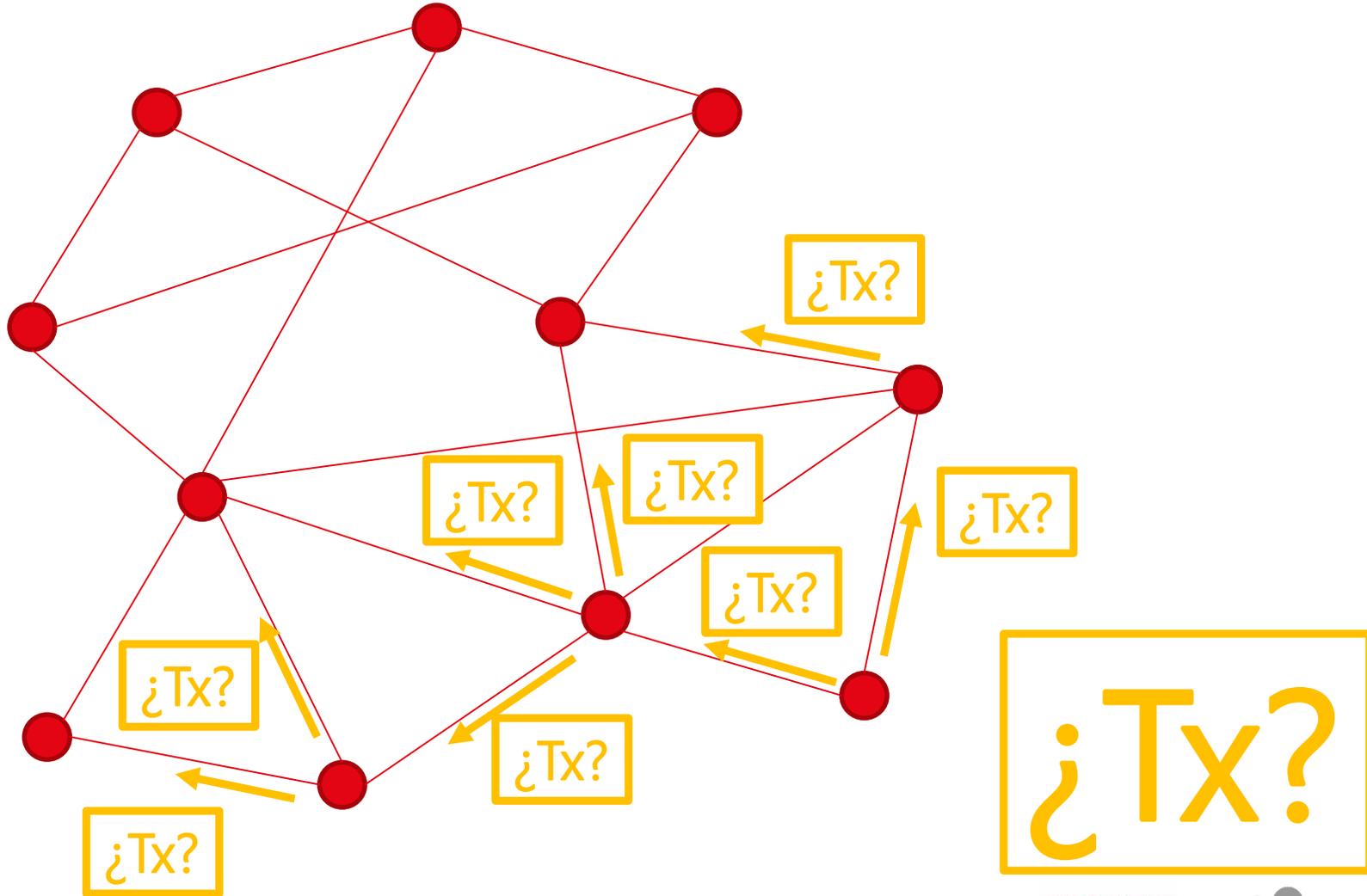
Protocolo de comunicación y consenso

Los nodos pueden disparar transacciones (generalmente a pedido de algún usuario externo)

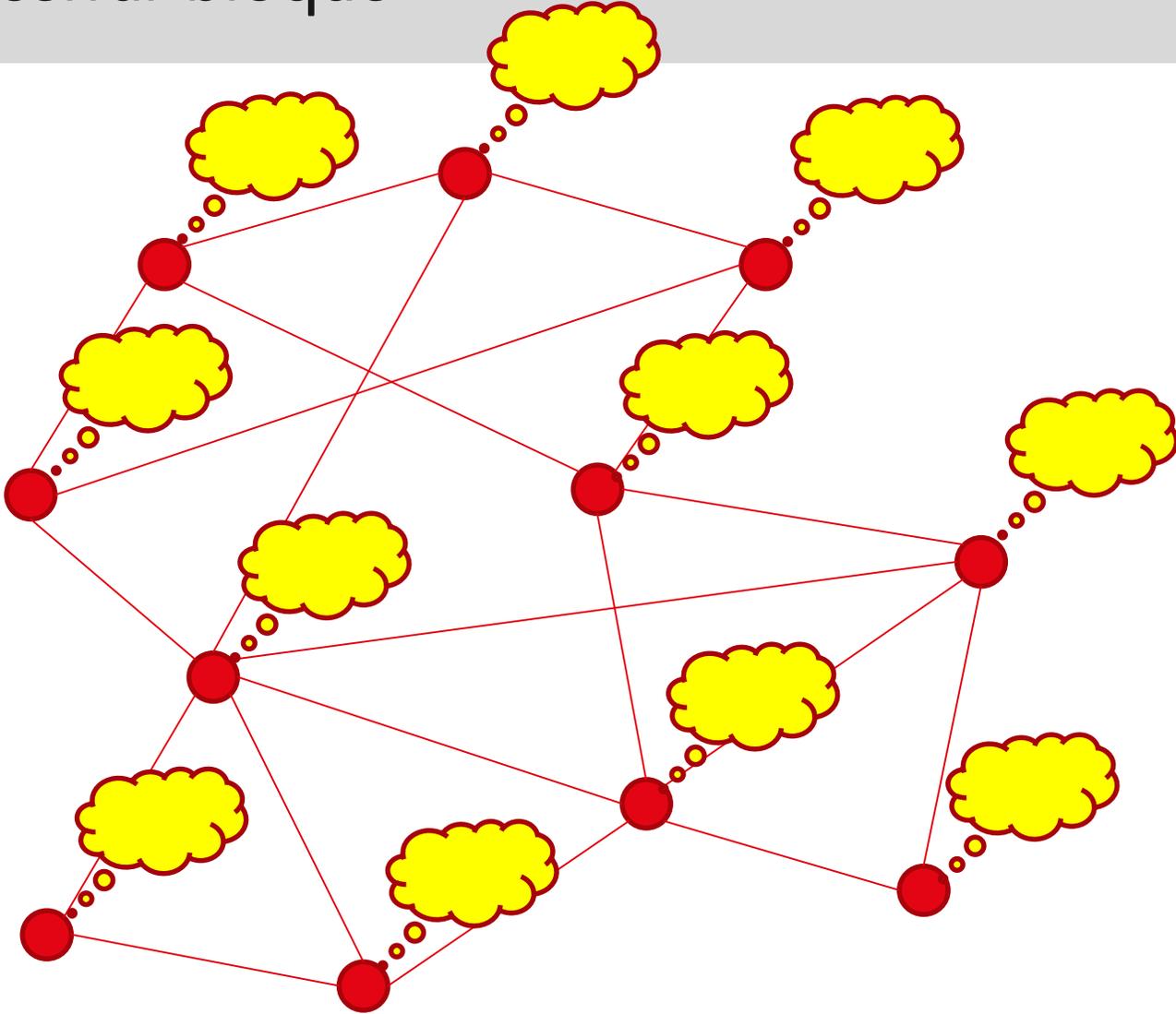


¿Tx?

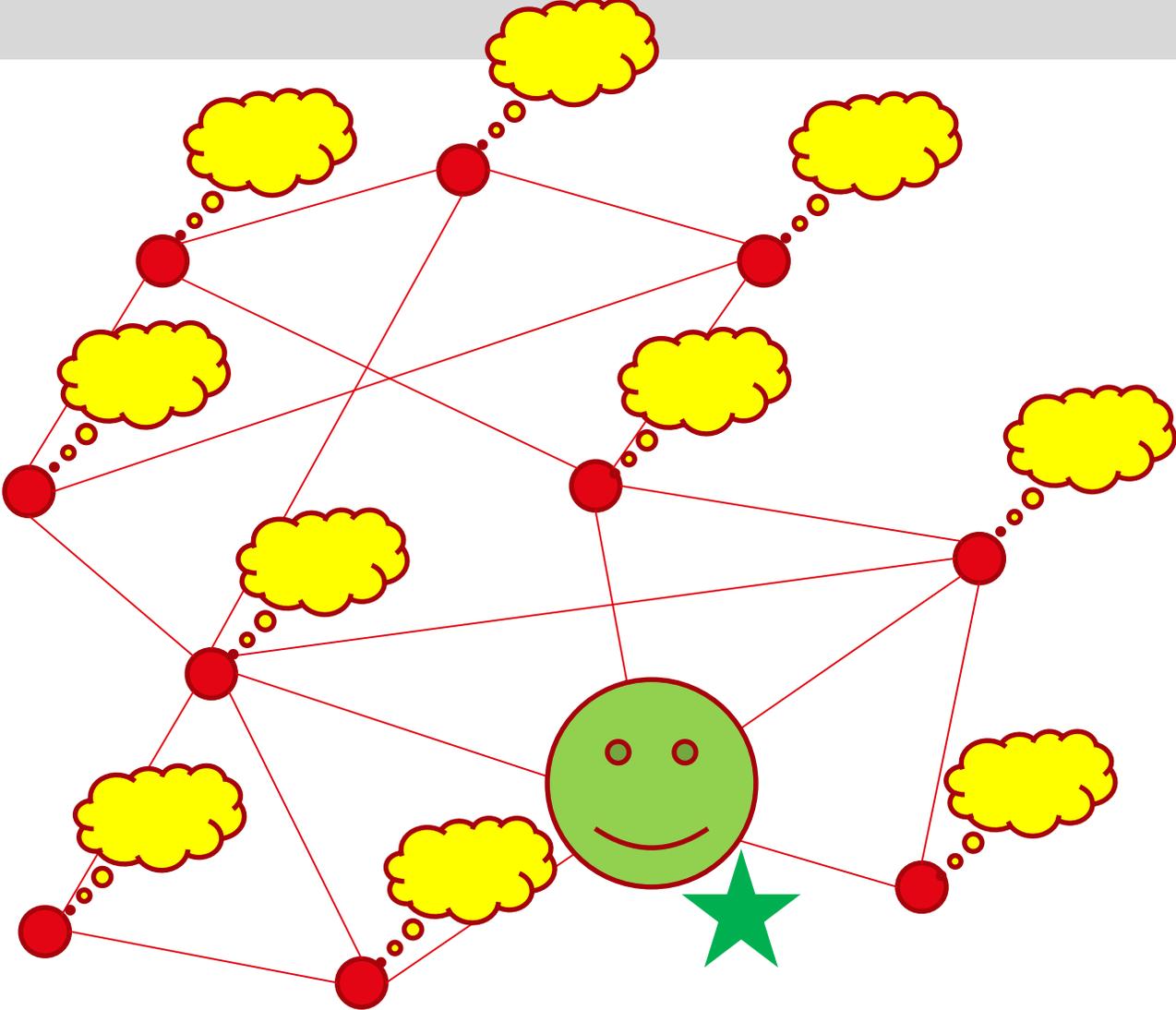
Transacción siendo validada



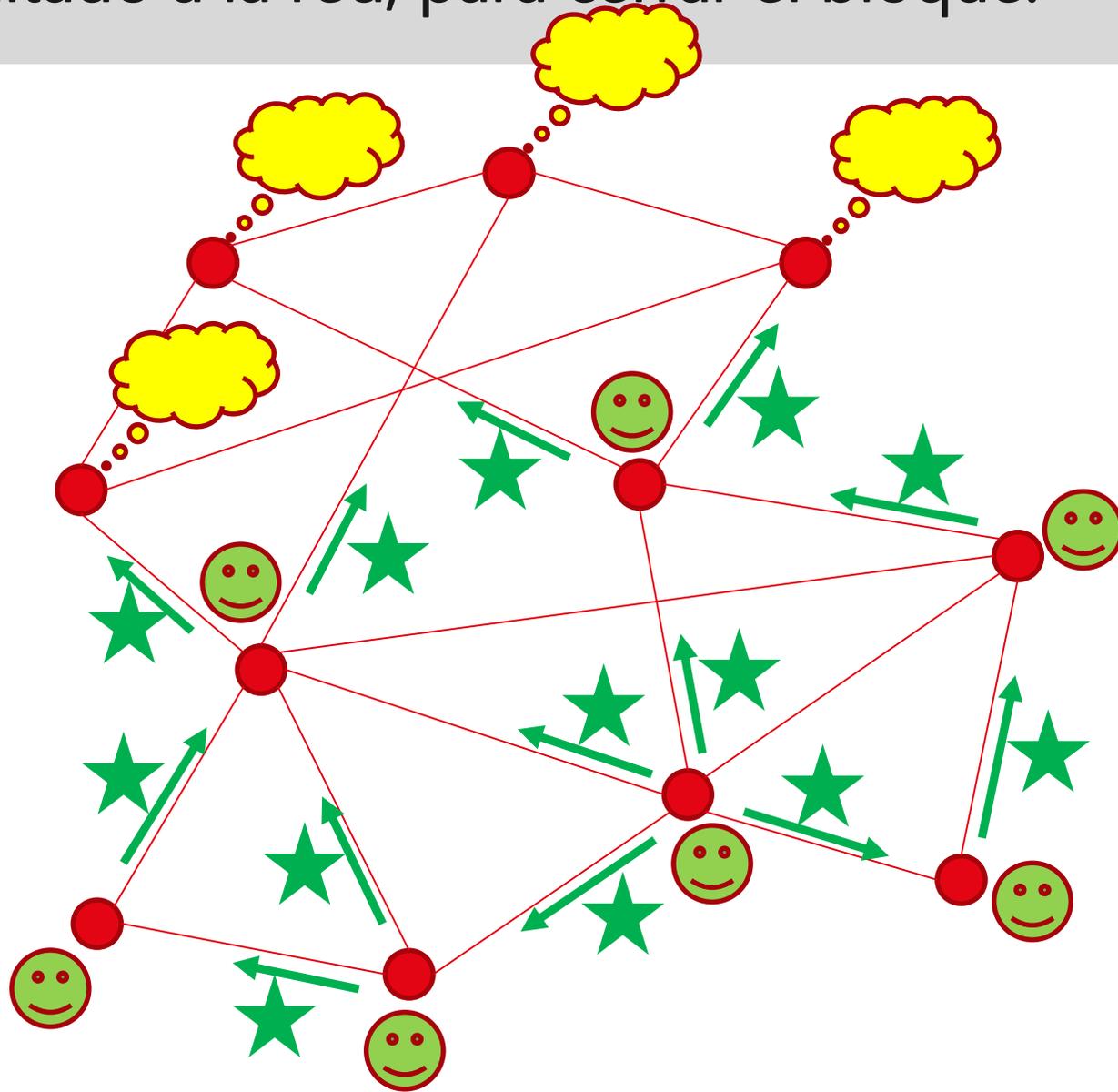
Desafío para cerrar bloque



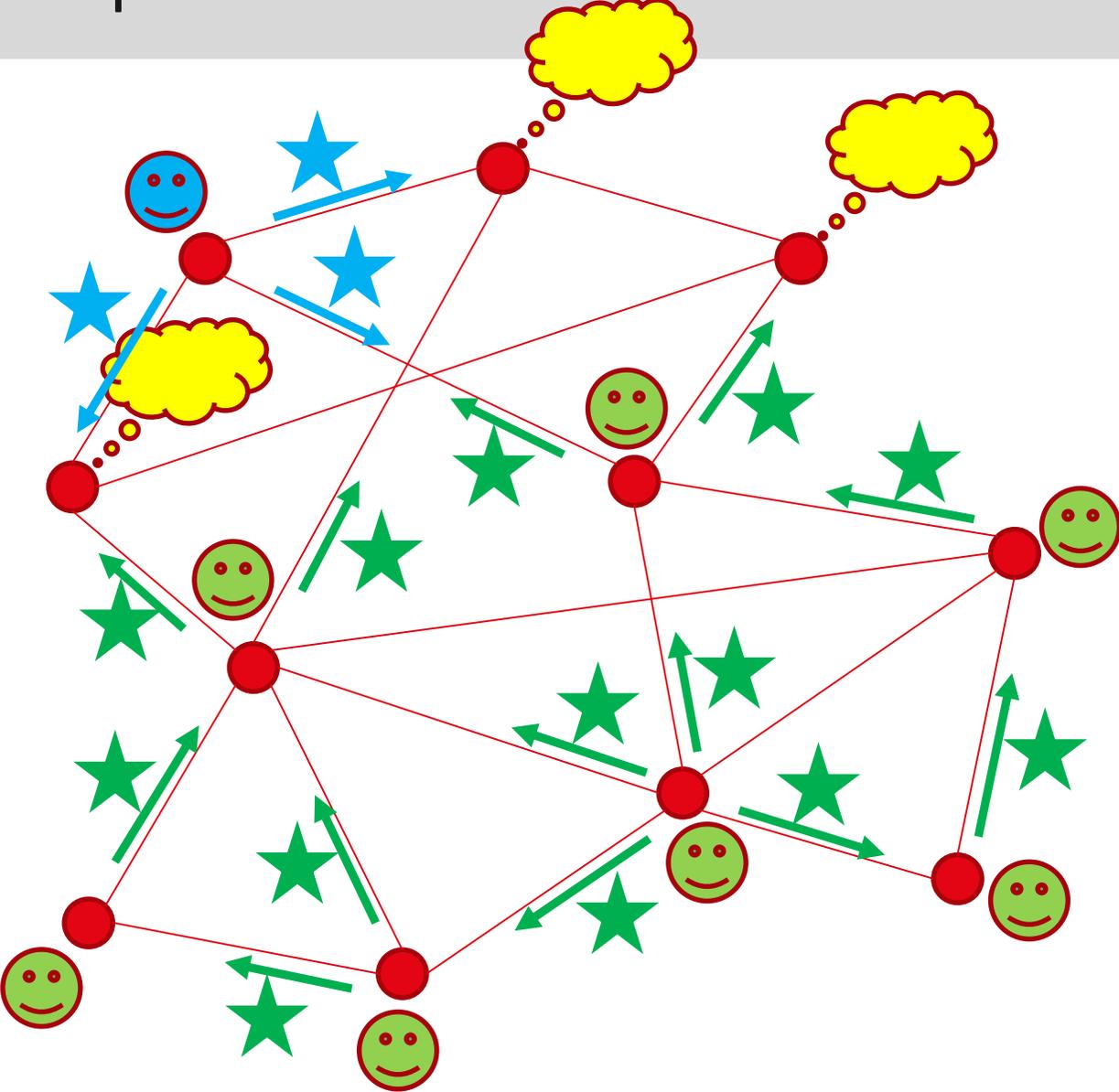
Quando un nodo resuelve el desafío...



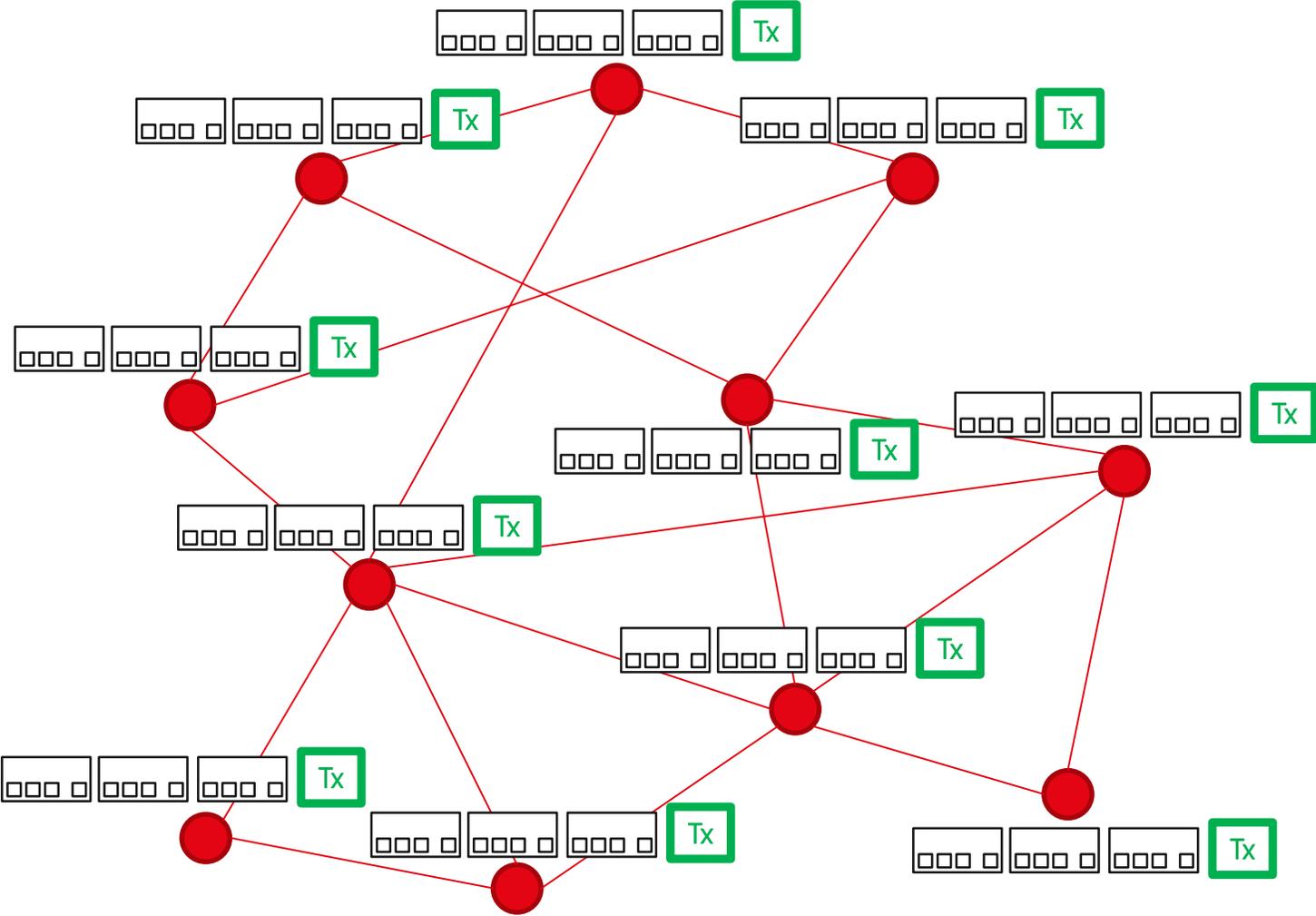
...envía resultado a la red, para cerrar el bloque.



Si hay conflicto por soluciones simultáneas. **CONSENSO!**



Transacción validada



El gran problema: **electricidad**



- Hay otros protocolos de consenso "más baratos".
- Se están proponiendo/desarrollando ideas para mejorar esta y otras cuestiones.



El ecosistema actual

Contratos inteligentes



Qué es un contrato inteligente?



- Blockchain denominada Ethereum:
 - Define una máquina virtual (**EVM**)
 - Cada nodo corre un lenguaje Turing-completo
 - Se pueden hacer **programas** -> **contratos inteligentes**
 - Motto tradicional: Code is Law



Stakeholders del ecosistema

- Existen muchos jugadores interesados (todos fuertes):
 - **Desarrolladores "de la VM"**: crean el software base para el consenso.
 - **Desarrolladores de "contratos"**: crean el software "de aplicación".
 - **Nodos (mineros)**: realizan los consensos, validan transacciones.
 - **Inversores**: poner dinero como "resguardo de valor" (los precios suben).
 - **Usuarios de contratos**: realizan transacciones, le dan vida al sistema.
 - **Investigadores / innovadores**: hacen crecer la tecnología.



El ecosistema actual

Aplicaciones existentes, en desarrollo y futuras



Real estate



https://www.dubailand.gov.ae/English/Pages/Blockchain.aspx



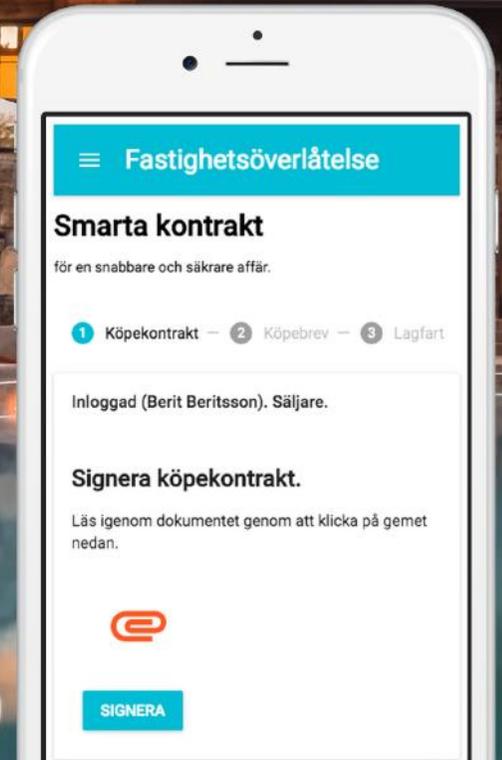
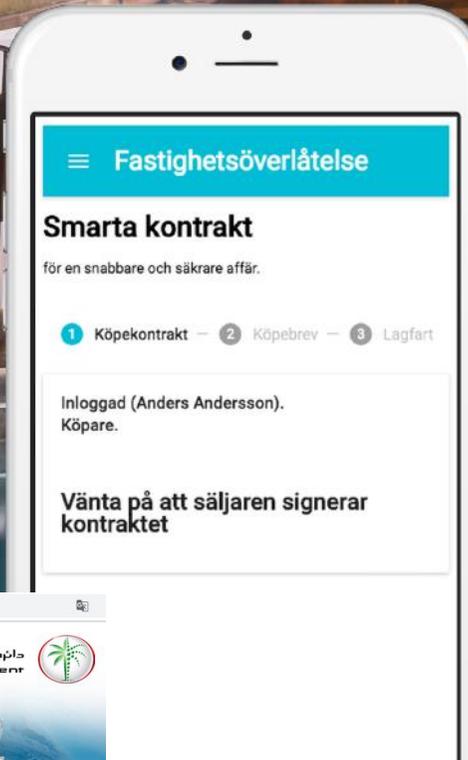
> Dubai Land Department > Blockchain Project

Blockchain Project

Dubai Land Department employing conscience based private network to automate and optimize end-to-end real-estate business process using the Blockchain technology. A Blockchain is a distributed database that maintains a continuously growing list of records, called blocks, secured from tampering and revision. Each block contains a timestamp and a link to a previous block. By design, blockchains are inherently resistant to modification of the data once recorded; the data in a block cannot be altered retroactively. Dubai Land Department employing the blockchain in three initiatives (Ownership verification in DLD Mobile Application, Property sale by Developer and Smart Leasing Process) targeting the improvement of providing the services, improve the collaboration with other parties involved the real estate market and to create a secured digital assets.

Key Features:

- The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset
- Write end-to-end property transactions on to Real Estate Blockchain to provide scalable, secured, transparent, shared, immutable property data to all the participants of the trusted network.
- Eliminate paper documentation, replace with digital records, and digitally signed documents.
- Eliminate the manual processes by integrating required stakeholders that are participating in the process (Customer, developer, DEWA, Payment Channel, DM, DLD, DNRD etc.) through Blockchain network.
- Provide hybrid platform for real estate market to be shared across different government or private entities to get benefit of real-time data and avoid manual processes to complete the transactions by participants.
- Sharing the information between entities to serve the Open Data initiative.
- Improve, secure and simplify the overall property transaction processes.
- Increase Operational Efficiency.



تحدي البلوك تشين
BLOCKCHAIN CHALLENGE
A SMART DUBAI INITIATIVE

DUBAI BLOCKCHAIN CHALLENGE
DUBAI DESIGN DISTRICT | 29 - 30 MAY 2017

21 GLOBAL START UPS

\$45,000 PRIZE MONEY

JUDGES, INVESTORS, INFLUENCERS

SMART DUBAI 2021
PREPARING DUBAI TO
EMBRACE THE FUTURE,
NOW

DUBAI DATA
DUBAI DATA ECONOMIC
IMPACT REPORT

SMART DUBAI INITIATIVE
HAPPINESS METER OPEN
FOR PRIVATE SECTOR

HAPPINESS AGENDA
THE FIRST INTERNATIONAL
HACKATHON FOR
HAPPINESS

SMART DUBAI INITIATIVE
BLOCKCHAIN CHALLENGE

Videojuegos



My Tamagotchi Forever

Elección del editor

BANDAI NAMCO Entertainment Europe
Juegos ocasionales

★★★★☆
32,268

E Todos

Contiene anuncios

Esta app es compatible con todos tus dispositivos.

Agregar a la lista de deseos

Instalar



Videojuegos (CryptoKitties)



DIGITAL TRENDS

Now Reading: Cat got your wallet? CryptoKitties virtual feline fetches \$170K in crypto c



SHARE



Chuong Nguyen

POSTED ON
9.5.18 - 2:04PM

COMPUTING

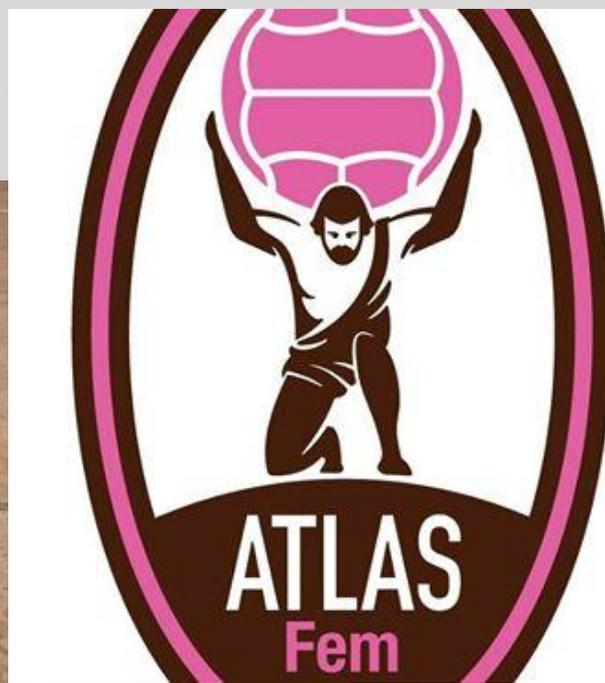
Cat got your wallet? CryptoKitties virtual feline fetches \$170K in crypto cash



[CryptoKitties](#), an Ethereum blockchain-based game that allows users to breed, trade, and sell digital cats, may have scored the most expensive in-app purchase to date with the sale of a CryptoKitty named Dragon for approximately \$170,000, or the



Atlas (la otra pasión)



https://web.telegram.org/#/im?p=@atlas_camisetas_bot

Otros diversos



- En US, hay **más de 1000 start-ups** haciendo cosas sobre blockchain.

Forbes

Billionaires Innovation Leadership Money Consumer Industry

A Medium Corporation [US] | <https://medium.com/coinmonks/25-blockchain-startups-to-watch-in-2018-2019-infographic-113b4d8f1b19>

M |  Coinmonks

HOME FILTER ▼ BLOCKCHAIN TUTORIALS CRYPTO ECONOMY SMART CONTRACTS DAPPS DONATE ↗ WRITE FOR US | FORUM 🔍

25 blockchain startups to watch in 2018–2019 (infographic)



45,880 views | Jul 10, 2018, 09:32am

Top 10 New Blockchain Companies To Watch For In 2018



Andrew Rossow Contributor ⓘ

Personal Finance

I cover digital money & blockchain technology: but watch your privacy



COMPANY SERVICES INDUSTRIES CAREERS BLOG CONTACT US

 +972-72-211660



51 Leading Blockchain Startups to Watch for 2018

Algunas **startups argentinas**



- **Bitex** (exchange internacional)
- **Ripio** (billetera virtual)
- **Voxelus** (VOX, dinero para jugar)
- **Decentraland** (simil Second Life)
- **Zeppelin** (verificación de seguridad en contratos inteligentes)
- **UTN Santa Fe** (registro de procesos organizacionales)

Hay mucho por hacer...



“El valor de mercado es de $200 \cdot 10^9$ USD,
pero el valor generado mucho menor. ”

(Vitalik Buterin, agosto 2018)



- El blockchain representa una **disrupción única global**.
- Mucha gente puede beneficiarse (**win-win**).
- Existen muchos intentando **innovar** con el blockchain.
- **Todavía no apareció** el Google / Facebook / Android de blockchain
- Las **posibilidades** son **infinitas** y, sobre todo, **desconocidas**.