BLOCKCHAIN CATALUNYA

BLOCKCHAIN, QUINA REVOLUCIÓ?

Jordi Herrera Joancomartí
Vicepresident de l'Associació Blockchain Catalunya
Professor de la UAB

22@ NETWORK BCN

Preguntes sobre la tecnologia Blockchain

- Què és?
- Per a què serveix?
- És una revolució?
- On es pot aplicar?
- Quines limitacions / reptes tecnològics té?

Què és?

- Una **blockchain** és una base de dades horrible amb uns retards d'escriptura exageradament alts i amb unes capacitats de cerca encara pitjors.
- Una **blockchain** és un registre transaccional ordenat seqüencialment amb la propietat d'integritat i en el qual només es permet afegir-hi informació.
- La **tecnologia blockchain** inclou tots els mecanisme, tècniques i procediments per proporcionar a una blockchain integritat i la propietat de "*només-permetre-afegir*".

La fragilitat de les definicions

- Què vol dir: **no es poden modificar** les transaccions d'una blockchain?
  - *Fins a quin punt una blockchain és immutable?*
  - *Sota quin concepte no es poden modificar? Sota cap concepte: mai? Només en casos extrems? Qui determina els casos extrems?*
  - *Qui no pot modificar-les? Ningú? Alguns usuaris concrets sí que poden?*
- Què vol dir: la blockchain té la propietat de **només-permetre-afegir** transaccions?
  - *Qui pot afegir-hi transaccions? Tothom? Només un grup específic d'usuaris? Un únic usuari?*
  - *Tothom pot veure les transaccions incloses? Només un grup d'usuaris? Cadascú les "seves"?*

Solucions existents que implementen les definicions anteriors

Depenent de les respostes a les preguntes anteriors tenim diferents tipus de blockchain:

- Permissionless (open) blockchains: tothom pot llegir i escriure-hi. Màxima transparència i màxima resistència a censura. (p.e. Bitcoin, Ethereum,...)
- Permissioned blockchains: només certs usuaris poden llegir i escriure informació. Necessitat d'identificació i de rols d'usuari. (p.e. Hyperledger Fabric, Multichain,...)

i els mecanismes per assegurar-ne les propietats són molt diferents.

Quina revolució suposa la tecnologia blockchain?

La tecnologia blockchain és trencadora i disruptiva en tant que permet **descentralitzar processos de forma segura.**

- Això obre les portes a:
  - *Reduir la intermediació.*
  - *Eliminar posicions dominants.*
  - *Augmentar la transparència dels processos.*
  - *Incrementar la seguretat d'un sistema.*
- El preu de descentralitzar de forma segura és, sovint, l'eficiència!

On es pot aplicar?

- Com a registre transaccional, la tecnologia blockchain es pot aplicar pràcticament a qualsevol domini.
- Qualsevol aplicació que necessiti un registre transaccional és susceptible a poder fer servir una blockchain.
- Per tant, la pregunta correcta a fer-se no és aquesta!

Per què es vol utilitzar?

Quins avantatges m'aporta aquesta tecnologia respecte a qualsevol altra?

- Vull eliminar la intermediació?
- Em cal reduir posicions dominants en els meus processos?
- L'increment en la seguretat del meu sistema queda compensat per la pèrdua d'eficiència?
- Necessito mostrar una transparència en el registre de les transaccions?

Quines limitacions / reptes té?

- La tecnologia blockchain està a les beceroles, tot just comença a resoldre alguns problemes de base:
  - *Escalabilitat*
  - *Privadesa*
  - *Digitalització del món real: necessitat d'oracles*
  - *“Longevitat”*

BLOCKCHAIN CATALUNYA

PREGUNTES?

Jordi Herrera Joancomartí
Vicepresident de l'Associació Blockchain Catalunya
Professor al Departament d'Enginyeria de la Informació i les Comunicacions - UAB

@joancomarti

22@ NETWORK BCN