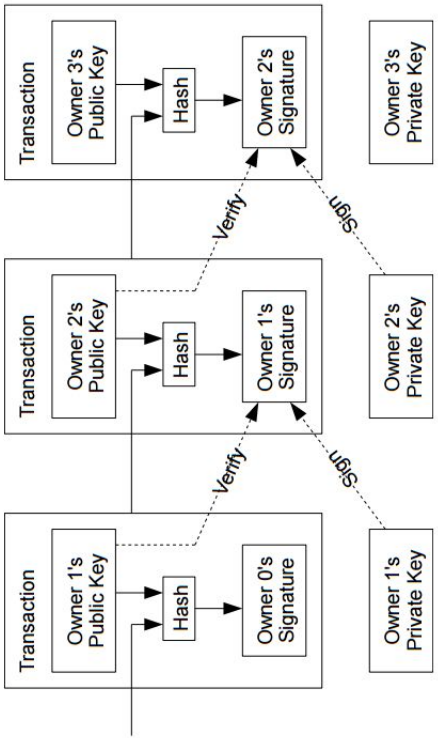
Il ruolo delle università nello sviluppo di tecnologie e infrastrutture blockchain per servizi pubblici



Peer to peer electronic cash

Nel 2008 il misterioso Satoshi Nakamoto inventa Bitcoin, un meccanismo per lo scambio di asset digitali:

- Tra attori pseudonimi (ID crittografica)
- Programmabile

Le transazioni vengono registrate in una **blockchain:**

- Registro append-only
- Quali transazioni vengono incluse? In che ordine?
- Un meccanismo di consenso garantisce convergenza e stabilità in modo distribuito (non serve attore “onesto”)

Programmabilità

- Nel 2014, il progetto Ethereum generalizza Bitcoin, introducendo programmabilità Turing completa
- Possible descrizione: un “world computer” in cui...
  - Chiunque può caricare del codice
  - Il codice caricato è pubblico, non modificabile, non interrompibile
  - Il codice può gestire (ricevere/inviare) asset digitali
- Applicazioni:
  - Finanziarie
  - Asset digitali (token)
  - Meccanismi di coordinamento basati su valore economico
- Bonus: massima interoperabilità tra applicazioni

Interesse per pubblica amministrazione

La digitalizzazione dei processi:

- Abbassa i costi
- Aumenta la velocità
- **Non** aumenta la trasparenza (l'autorevolezza) dei processi
- Interoperabilità problematica

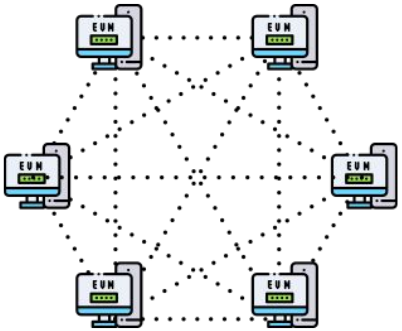
Es: chi mi dice che una graduatoria è stata calcolata correttamente?

Blockchain => processi digitali *evidentemente* corretti (seguono regole pubbliche)

Possibili applicazioni pubbliche:

- Gestione di identità digitale (esempio PKI, revocation list)
- Procurement
- Politiche economiche di sostegno
- Meccanismi di incentivazione (esempio carbon credit)

Quale infrastruttura?



Quale infrastruttura per i servizi pubblici?

Ethereum? (public permissonless)

Suggestivo, ma:

- Costi non predicibili (legati a valore di ether e a congestione rete)
- Controllo da parte dei validatori (Miner Extractable Value)
- Sostenibilità ambientale del proof of work (anche se è in corso migrazione a PoS)

Proposta alternativa

- Infrastruttura *permissioned* con validatori istituzionali
- Esempio: European Blockchain Service Infrastructure (EBSI)

EBSI

EBSI sarà un’infrastruttura blockchain europea

Ogni stato membro avrà almeno un nodo validatore

In Italia al momento ci sono Polimi, INPS, Infratel

EBSI potrà essere la struttura di riferimento per applicazioni pubbliche cross-border

Data la dimensione, è difficile sperimentare lungo alcune direttrici

Obiettivi

IBSI è un progetto di ricerca che si propone di indagare diversi problemi:

- Che caratteristiche deve avere una rete blockchain per servizi pubblici?
  - Chi può caricare programmi (deploy di smart contract)?
  - Chi può accedere ai dati in lettura?
  - Chi devono essere i validatori? Quale deve essere il meccanismo di consenso?
- Quale può essere la governance? Come devono essere distribuiti i costi infrastrutturali?
  - E.g.: costo distribuito su responsabili delle applicazioni tramite il meccanismo del gas
- Come è possibile rispettare la privacy, ed essere GDPR compliant, in una rete in cui le info sono pubbliche?

Ruolo di Polimi (e ecosistema universitario in generale)

Il Politecnico:

- Ospita il principale osservatorio nazionale sul tema blockchain
- Partecipa già ad EBSI
- Attivo nella ricerca su problemi pertinenti (sistemi distribuiti, crittografia, cybersecurity, applicazioni, oracoli)
- Ha risorse culturali e competenze tecniche per contribuire fattivamente