# Time Based Proof of Stake

Takamaka.io
AiliA S.A.

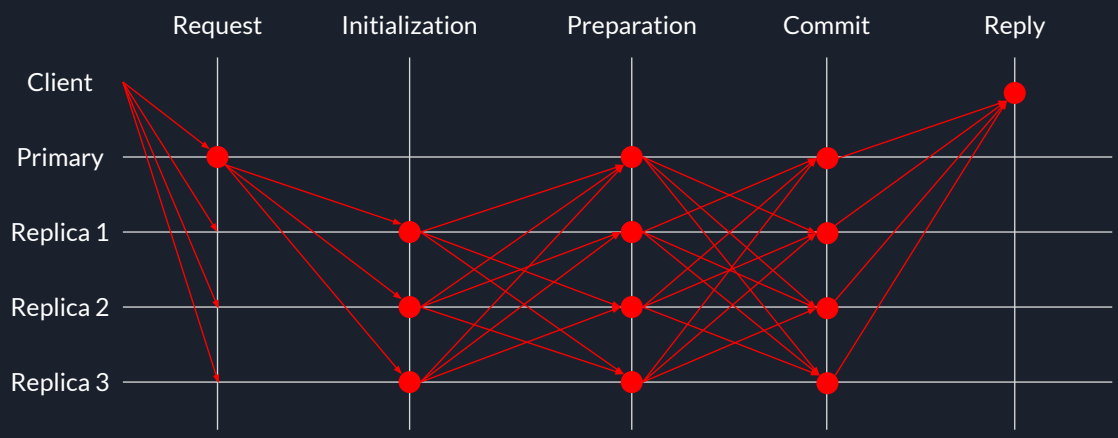
Giovanni Antino
Project Manager presso AiliA SA
https://www.takamaka.io

# pBFT

Barbara Liskov and Miguel Castro

- i nodi sono ordinati in sequenza
- i nodi sono divisi fra **primari** e **secondari**
- i nodi possono passare da primario a secondario e viceversa
- la decisione è presa a maggioranza
- il numero massimo di nodi malevoli è ⅓ della dimensione del network

# pBFT - complessità



# pBFT

- reattiva su insiemi ristretti di nodi
- per scalare richiede una gerarchizzazione
- l'aumento del livello di sicurezza è inversamente proporzionale alle performance
- richiede una gestione attiva dei nodi primari/secondari

# Requisiti per una nuova PoS

- Minimizzazione delle attività sul network
- Indipendenza decisionale dei nodi
- Bilanciamento del controllo
- Tolleranza del 50%+1 verso gli attori malevoli

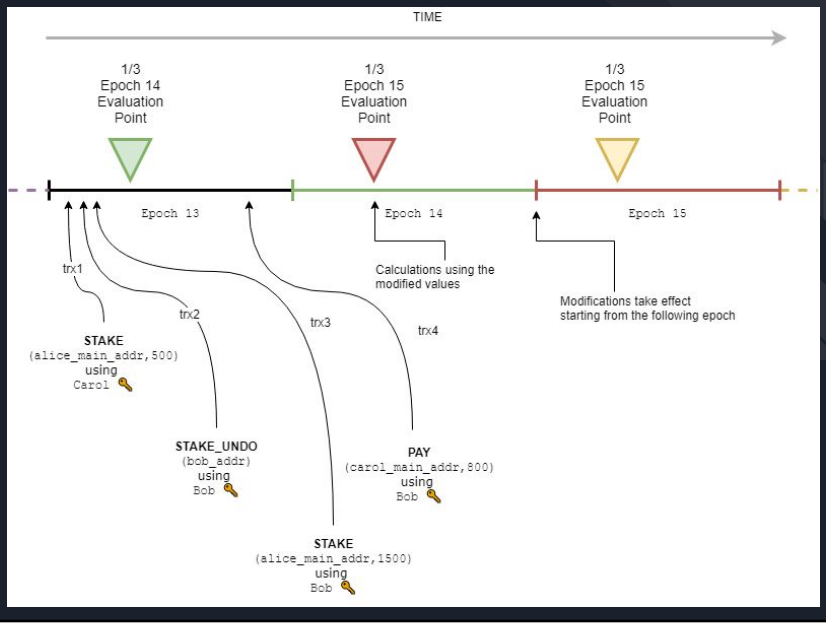
# Attori della TPoS

- **Nodi di mining**: server che eseguono il protocollo e hanno diritto di voto
- **Nodi di replica**: server che eseguono il protocollo ma non detengono diritto di voto
- **Holder**: detentori dei token necessari ad operare sulla chain

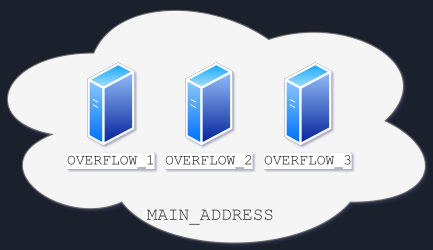
# Token della blockchain

- **Green Token**:
  - può essere utilizzato per attivare un nodo di replica come nodo di mining
  - da diritto a ricevere i reward
  - paga le operazioni sulla chain
- **Red Token**:
  - paga le operazioni sulla chain
  - non può essere usato per avere controllo sulla chain

# Epoch Evaluation

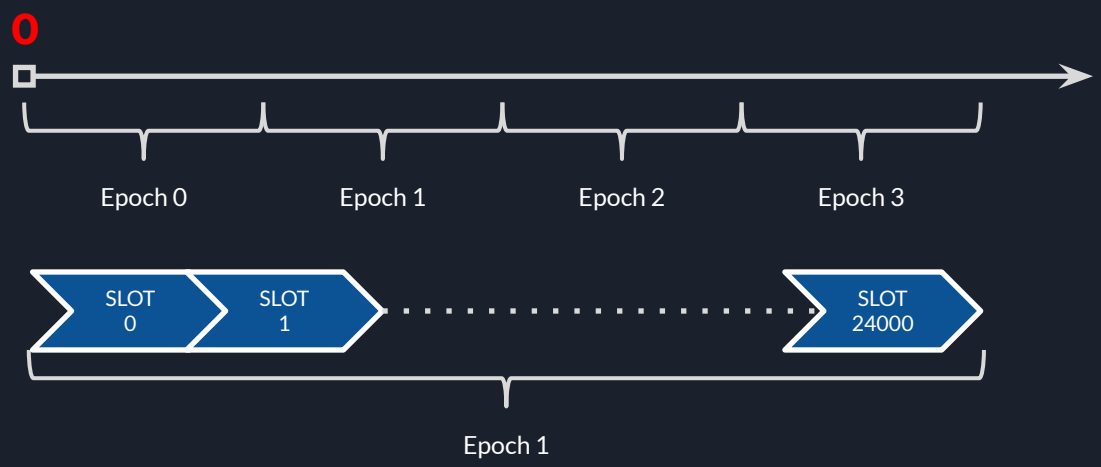



# Main vs Overflow

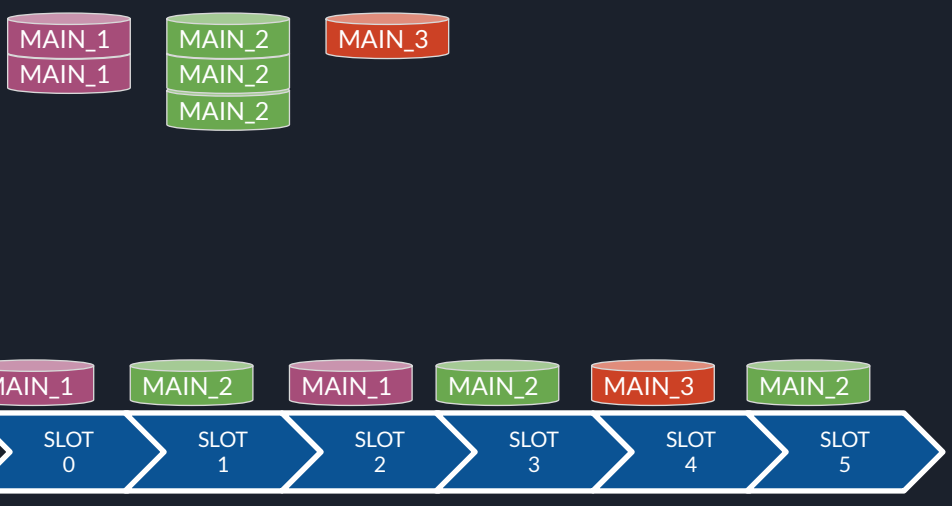



- Semplificare la gestione dei server
- Chiavi di management offline
- Mining pool
- Ridondanza

## Distribuzione del lavoro




## Distribuzione del lavoro



# Concentrazione della stake

- Efficienza → Minor numero di server
- Affidabilità → Maggior numero di server
- I Main non controllano le chiavi private degli holder
- Non posso impedire a chi ha tanta moneta di attivare tanti server

# Penalizzazioni

- **Attive**: es. coin slashing
- **Passive**:
  - mancata generazione del coinbase
  - congelamento dei fondi

# Penalizzazioni

- Impongo un numero massimo di slot per overflow → se ho molta stake devo attivare molti nodi fisici
- Per ogni blocco creato oltre il limite imposto:
  - niente coinbase
  - fee congelate per il doppio del tempo fuori dal limite

# Penalizzazioni

simulazione con dati reali

- Alice, alice_main_addr
  - node_a1, node_a2, … , node_a10
  - Stake 30.000
- Mallory, mallory_main_addr
  - node_m1
  - Stake 30.000
- Stake totale: 1.200.000
- Stake minima: 3.000
- Stake massima: 6.000
- Slot minimi: 60
- Slot massimi: **120**

# Penalizzazioni

simulazione con dati reali

- Stake totale: 1.200.000
- Stake minima: 3.000
- Stake massima: 6.000
- Slot minimi: 60
- Slot massimi: **120**

# Penalizzazioni

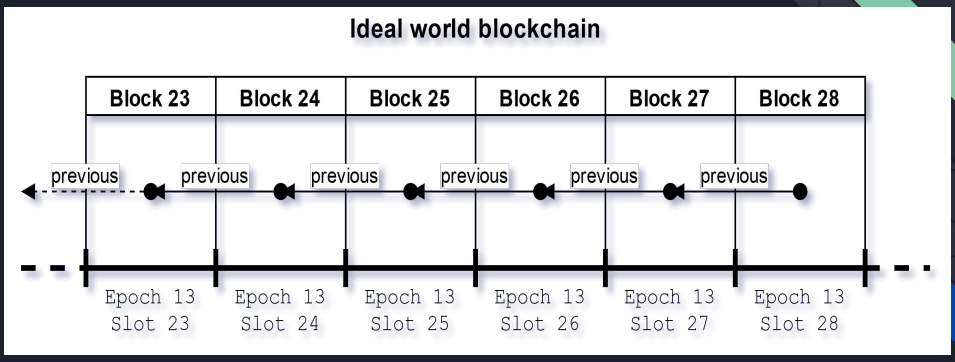
simulazione con dati reali

- Alice, alice_main_addr
  - node_a1, node_a2, … , node_a10 → 60 slot su 10 nodi
  - Stake 30.000 → 600 slot
- Mallory, mallory_main_addr
  - node_m1 → 600 slot
  - Stake 30.000 → 600 slot

# Penalizzazioni

| | Epoch 15 | Epoch 16 (attesa) | Epoch 16 (reale) | |
|---|---|---|---|---|
| **Alice** | 30.000 | 33.600 | 33.600 | Stake |
| | 600 | 600 | 601 (+1) | Slot assegnati |
| | 2,5% | 2,5% | 2,51% (+0,01) | Controllo del network |
| **Mallory** | 30.000 | 33.600 | 30.720 | Stake |
| | 600 | 600 | 550 (-50) (-8,33%) | Slot assegnati |
| | 2,5% | 2,5% | 2,29% (-0.21%) | Controllo del network |
| **Altri partecipanti** | 1.140.000 | 1.276.800 | 1.276.800 | Stake |
| | 22.800 | 22.800 | 22.849 (+49) | Slot assegnati |
| | 95% | 95% | 95,20% (+0,20%) | Controllo del network |

# Blockchain ideale

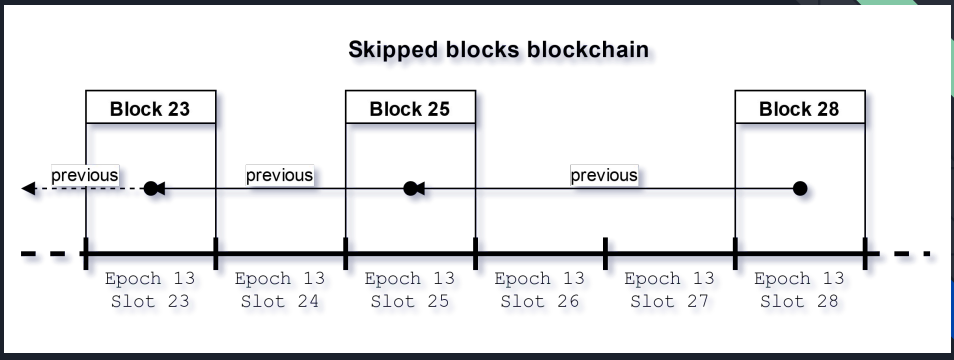


# Fork come comportarsi?

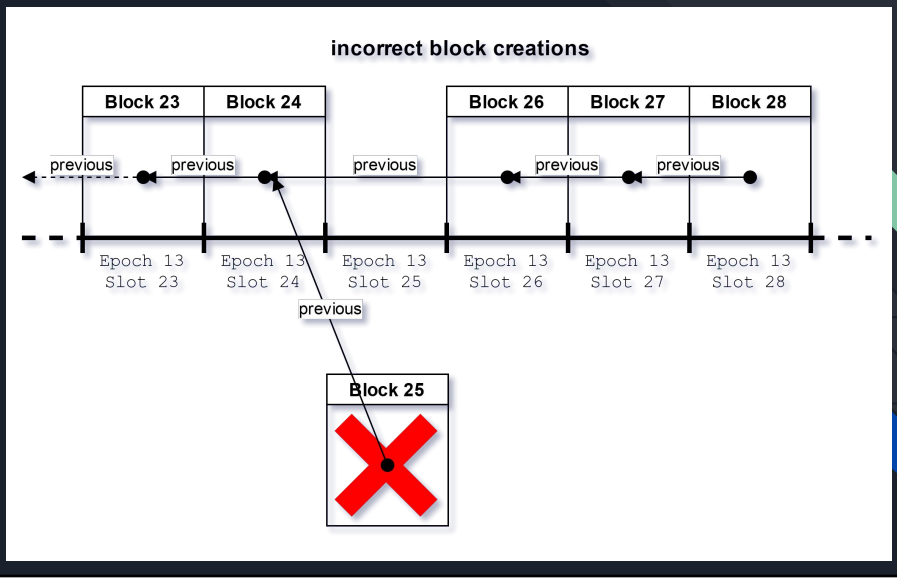
**Regola del peso massimo**

[Stake totale] / [numero degli slot]
=
[peso di uno slot]

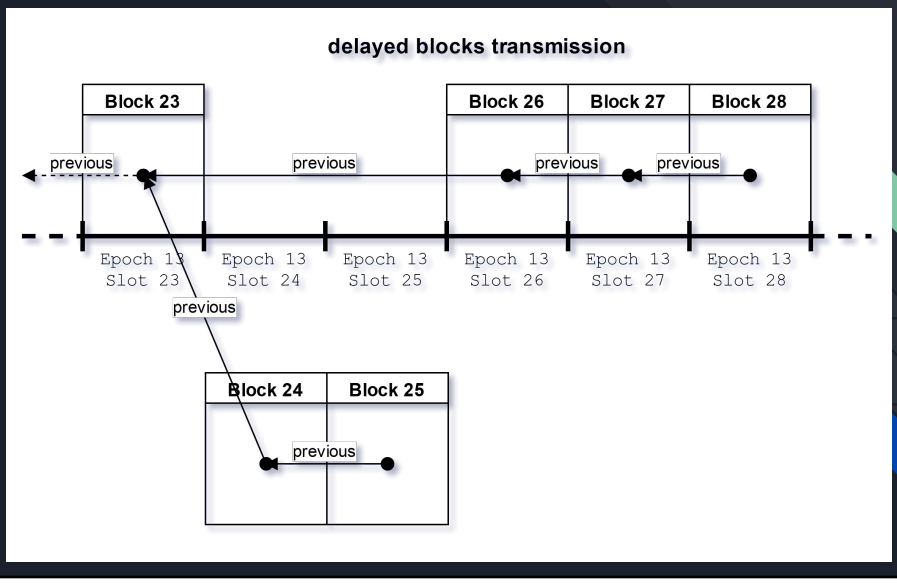
# Blockchain reale...



# Blockchain reale...




# Blockchain reale...



# Conclusioni

- Calcoli eseguiti in modalità greedy
- Client indipendenti nel calcolare il proprio stato interno
- 50%+1 livello di sicurezza
- Numero di messaggi lineari nel network

Takamaka

Takamaka.io

Grazie a tutti per il vostro tempo :-)