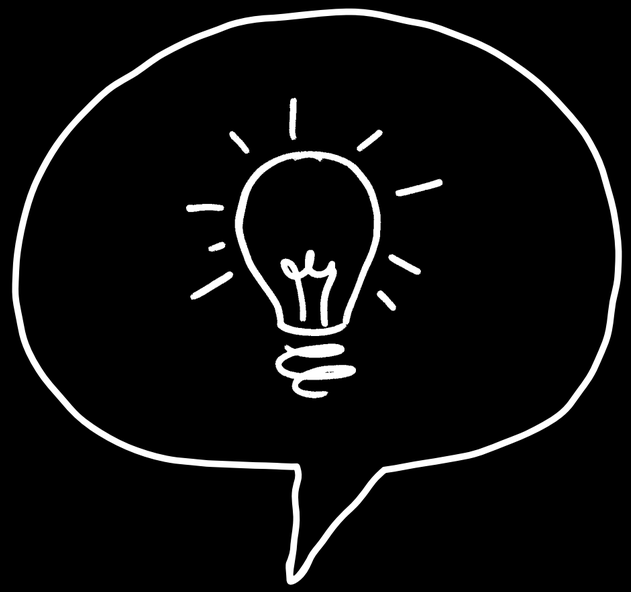
Koncenzus algoritmi

MERISA BEŠIROVIĆ



link do simulatora
https://simewu.com/blockchain-simulator/

Kako cvorovi komuniciraju i njihov zadatak

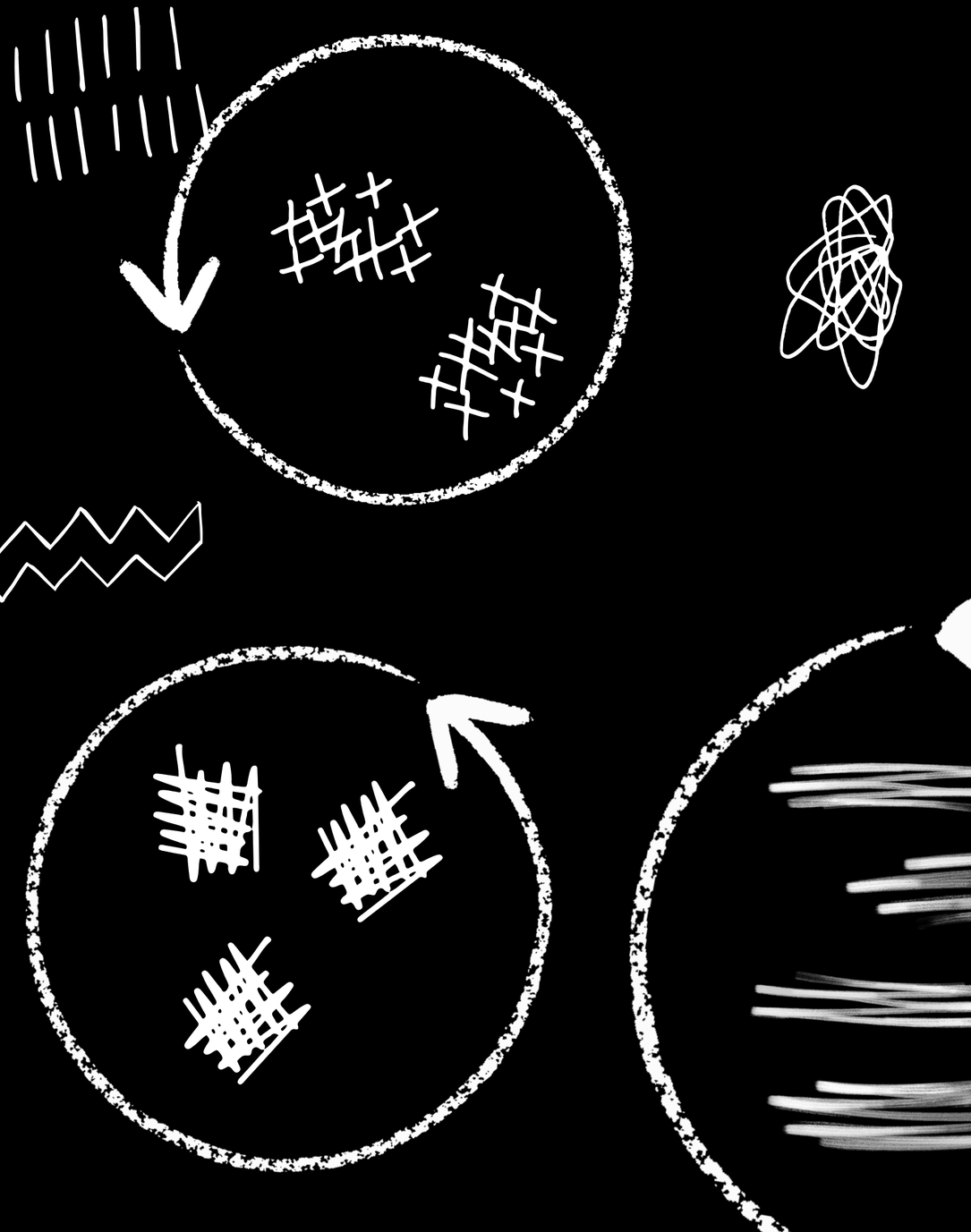
*ovlašćeni mrežni akteri i služe kao komunikacioni za razne mrežne zadatke

*full, light miner čvorovi

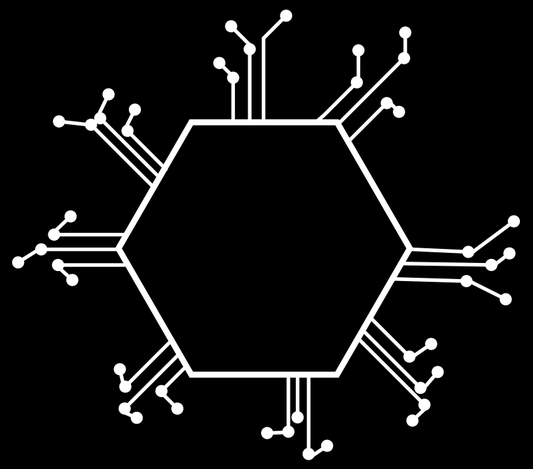
*zasebni entiteti i komuniciraju peer-to-peer - broadcast

*sinhronizacija čvorova

-ibd i odrzavanje



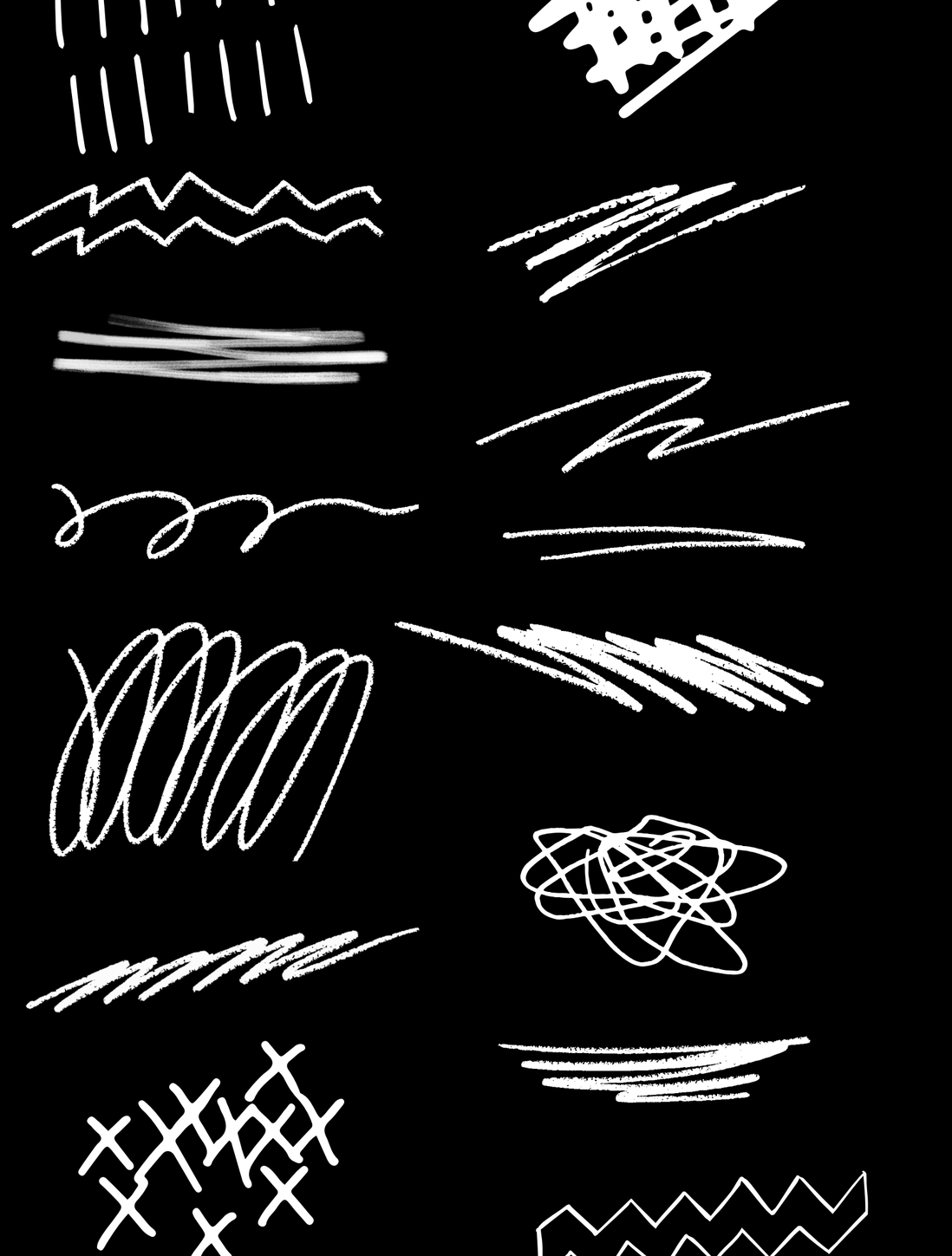
Šta su koncenzus algoritmi?



- Ne postoji centralno telo koje bi verifikovalo transakcije
- Verifikacija moguća samo zbog prisustva protokola konsenzusa

Zajednicki cilj algoritama

- postizanje sporazuma
- saradnja
- jednaka prava za svaki čvor
- obavezno učešće svakog čvora u procesu konsenzusa



Proof of work (POW)

Ledger

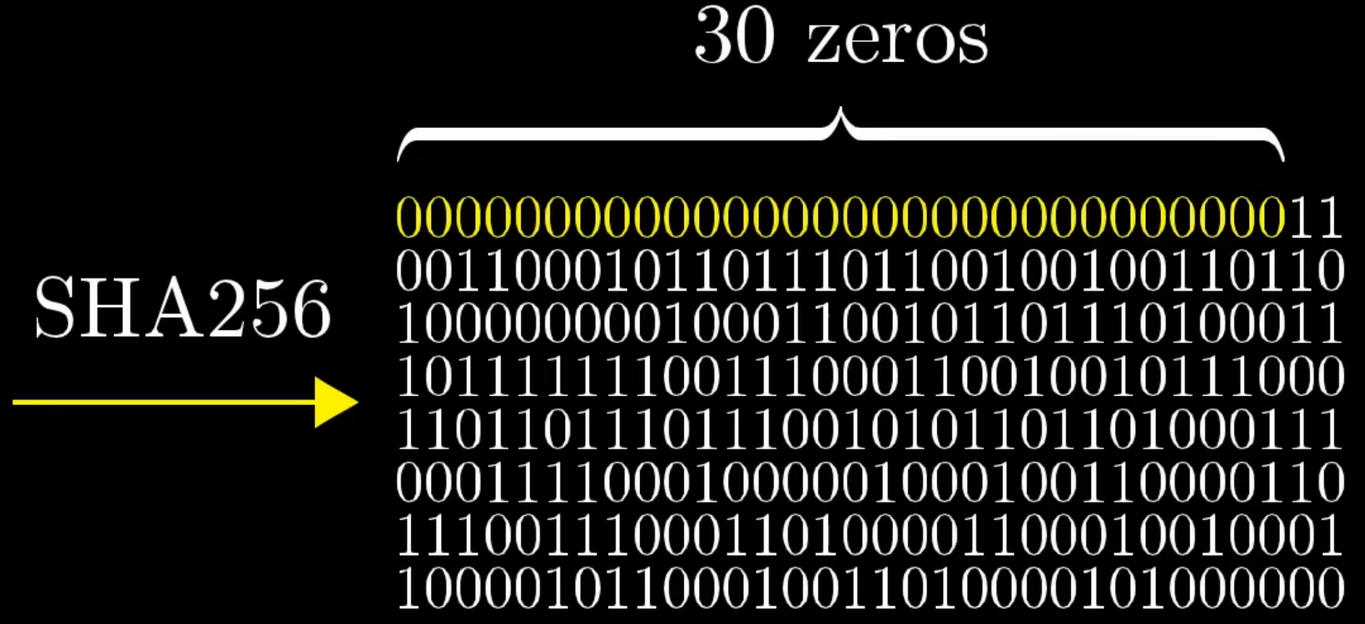
Alice pays Bob 20 LD

Alice pays You 30 LD

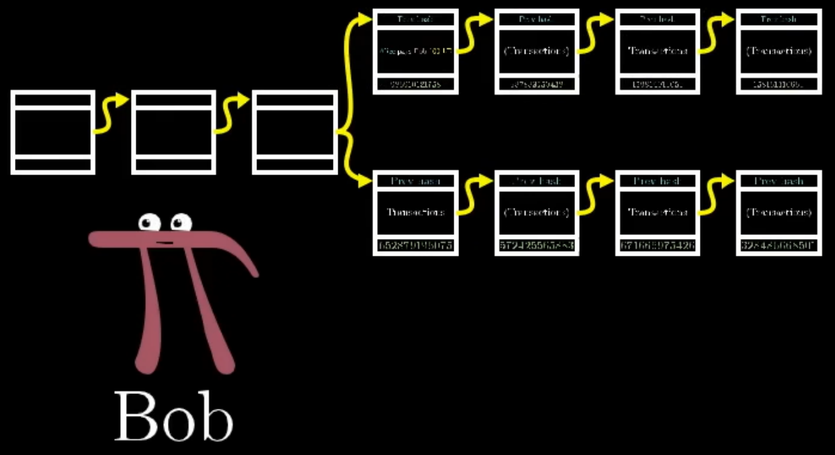
Charlie pays You 100 LD

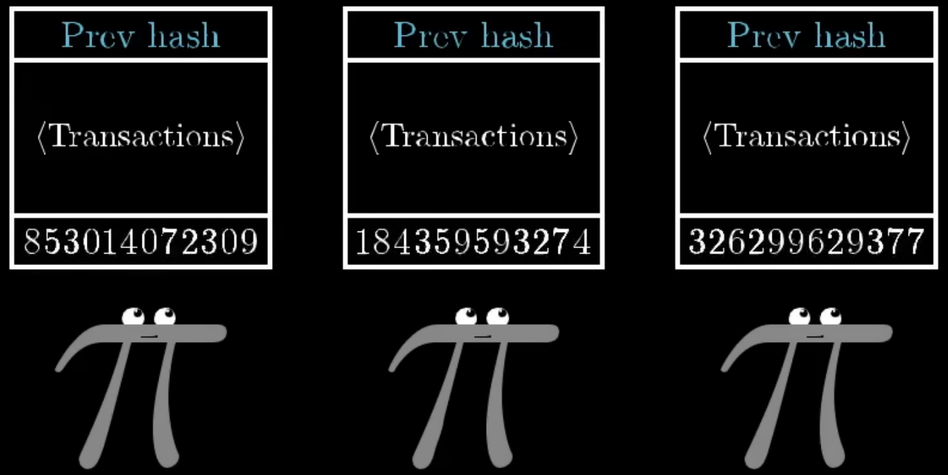
1073765433

SHA256



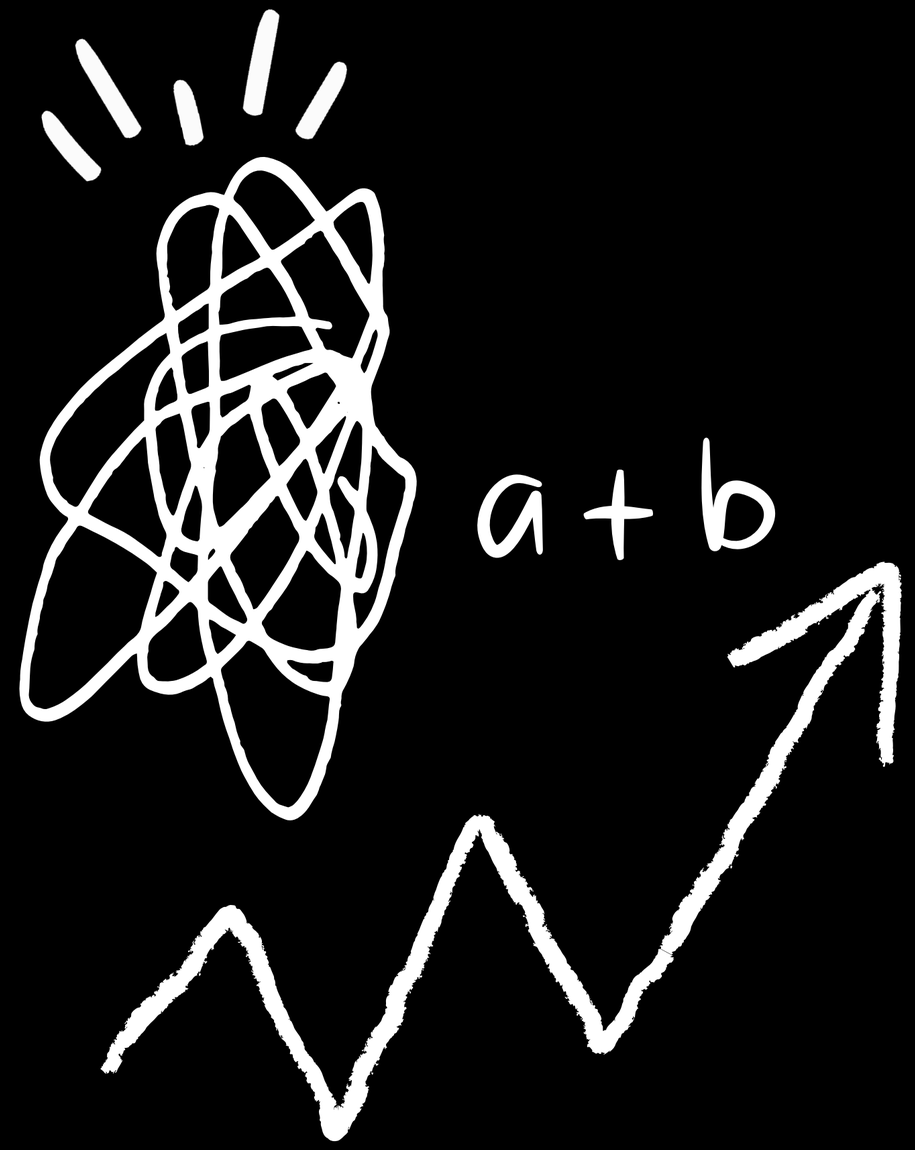
Koji chain je ispravan?





Problemi

1. Visoka potrošnja energije
2.Centralizacija rudarenja
3.Resursi
4.Potencijal za napade
51% napad

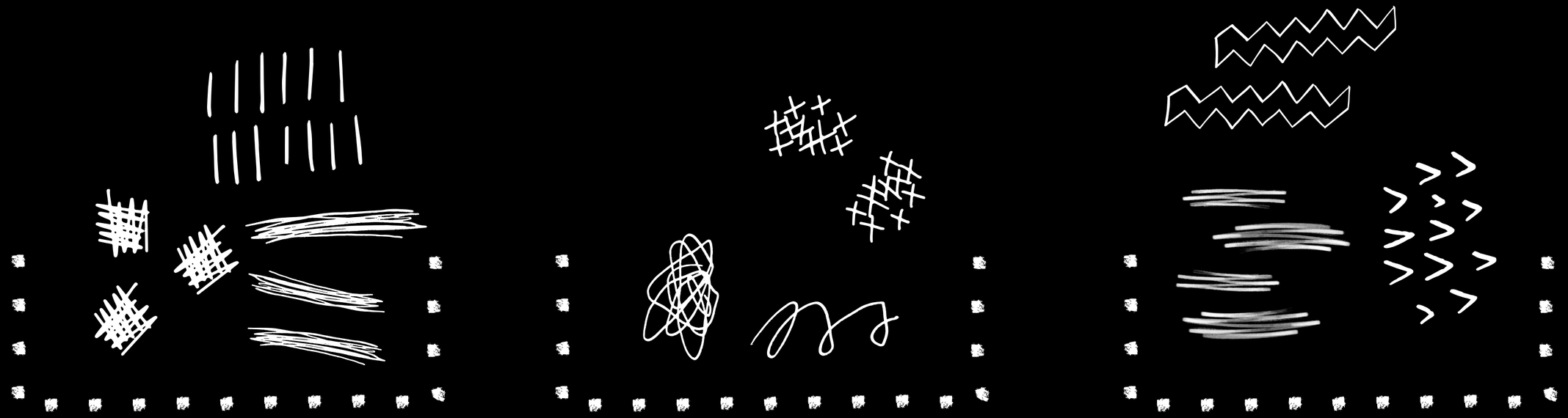


Proof of stake (POS)

- validatori blokova
- minting/forging
- ulog
- nevalidni blokovi – gube deo uloga
- nije potrebna posebna mining oprema

Problemi

- "Rich get richer" efekat
- Mogućnost za napade
- Smanjenje motivacije za transakcije



DPOS

- Delegirani čvorovi
- Rotacija delegata
- Glasanje korisnika
- Brza vremena blokiranja

1. **Proof of Burn (PoB):** Učesnici dokazuju svoju posvećenost sistemu tako što "spaljuju" (trajno uništavaju) određenu količinu kriptovalute,
2. **Practical Byzantine Fault Tolerance (PBFT):** Algoritam koji omogućava konsenzus među čvorovima u distribuiranim sistemima, gde se postiže saglasnost čak i ako određeni broj čvorova nije pouzdan ili ponaša se zlonamerno