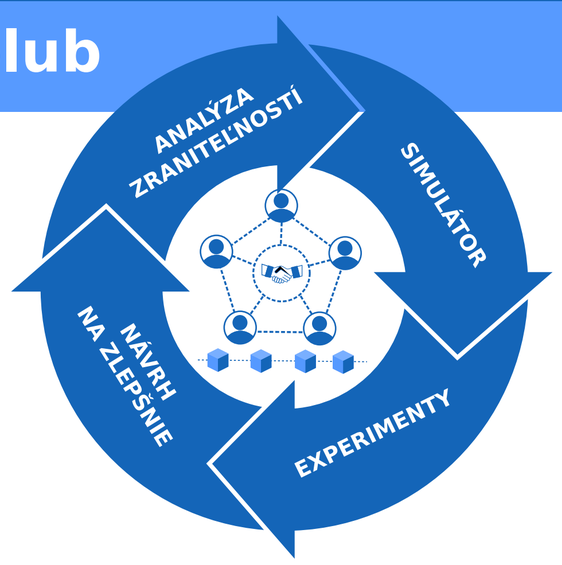
Testovanie bezpečnosti a výkonnosti blockchainu Harmony pomocou simulácie

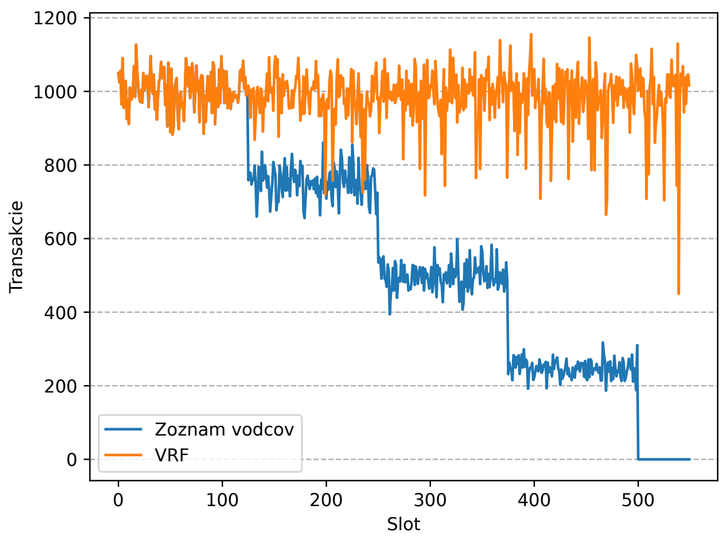
Juraj Holub

3



DoS útok

- Hlasovanie pomocou byzantskej zhody (2/3)
- Vodca a validátory
- Rozvrh vodcov
- Verifiable Delay Function (VRF)
  - Algorand
  - Nepredvídateľnosť vodcu

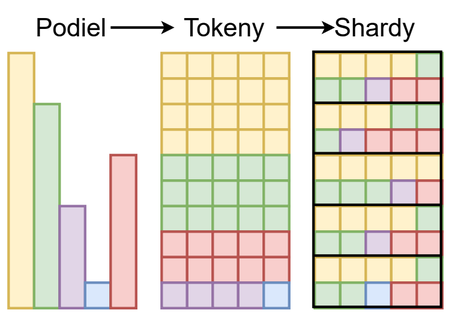


Obrázok 3. Porovnanie priepustnosti transakcií pri DoS útoku v prípade pôvodného rozvrhu vodcov a voľby vodcu pomocou VRF.

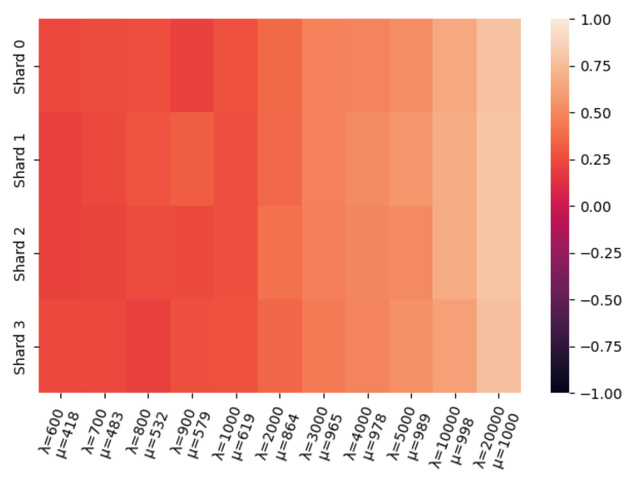
Sharding a Proof-of-Stake

- Škálovateľnosť
- Epocha
- Permutácia
- Distribuované generovanie náhodnosti
- Tokenizácia:

$$t = \frac{S_{e-1}}{n.\lambda}$$

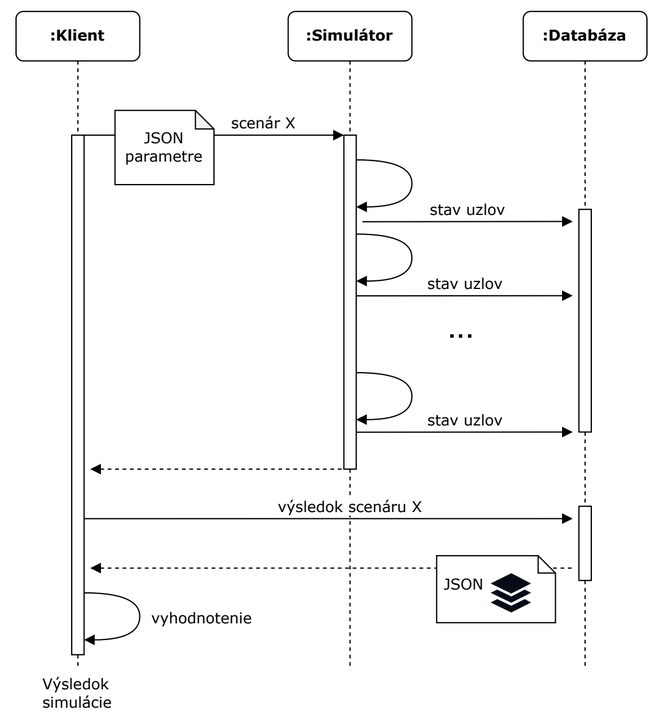


Obrázok 1. Rozdelenie hlasovacieho podielu medzi všetky shardy.



Obrázok 5. Teplotná mapa Spearmanovho korelačného koeficientu medzi skutočným podielom uzlov a hlasovacím právom v jednotlivých shardoch.

Vytvorený simulátor



Obrázok 1. Sekvenčný diagram procesu simulácie.

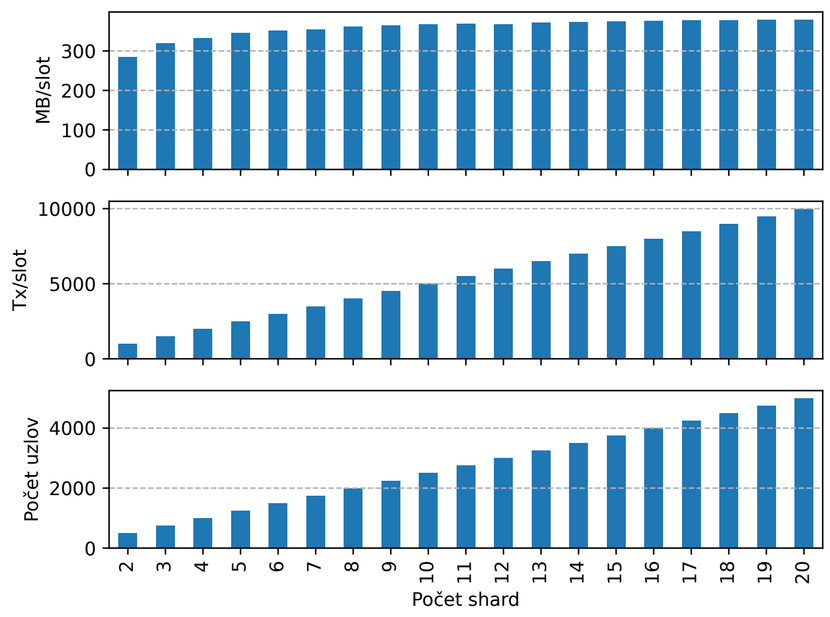
- **Klient**
  - Python konzolová aplikácia
  - REST API
- **Server**
  - Wittgenstein
  - MongoDB
  - Docker-compose

serveraddress:8080/harmony

```
{
    "epochDurationInSlots": 32_000,
    "numberOfEpochs": 100,
    "txSizeInBytes": 32,
    "blockHeaderSizeInBytes": 80,
    "networkSize": 1500,
    "numberOfShards": 4,
    "expectedTxPerBlock": 3000,
    "byzantineNodes": 50,
    "lambda": 600,
    "ddosAttack": False,
    "uniformStakeDistribution": True
}
```

Obrázok 2. Vstupné parametre simulácie.

Priepustnosť a škálovateľnosť

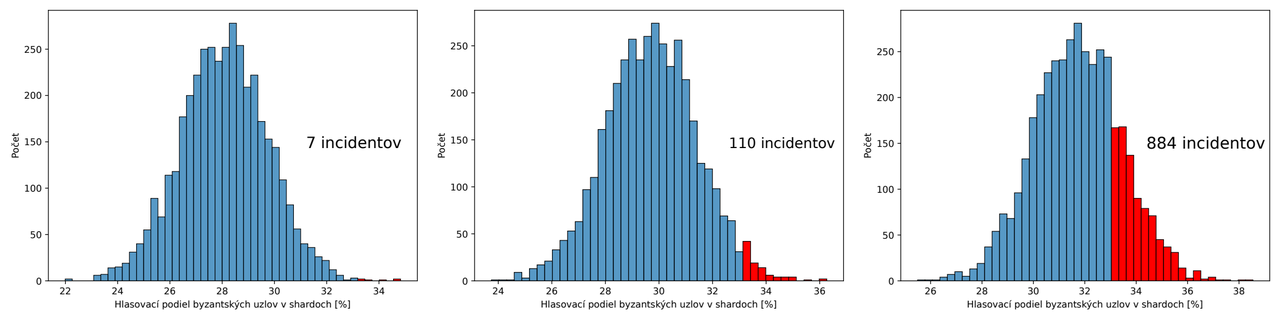


- 250 uzlov ≈ shard
- Transakcia 670B
- 600 TPS v každom sharde
- 1 Gbps linka ≈ 125MB/s
- 400MB/slot ≈ 3,2 sec

Obrázok 4. Priemerné množstvo dát prijaté každým uzlom v závislosti na veľkosti siete.

Útok na podskupinu uzlov

- Byzantské uzly vlastnia menej ako 1/3 podielu
- Prekazenie konsenzu
- 1000 epoch = 1000 redistribúcií do shardov
- Distribuované generovanie náhdnosti



(a) Byzantský podiel 28% **(b)** Byzantský podiel 30% **(c)** Byzantský podiel 32%

Obrázok 6. Histogram hlasovacieho podielu v shardoch.

Excel@FIT 2022