Usporedba performanci Ethereum raspodijeljene knjige na raznorodnom sklopovlju

Jakov Buratović

Mentor: prof. dr. sc. Igor Čavrak

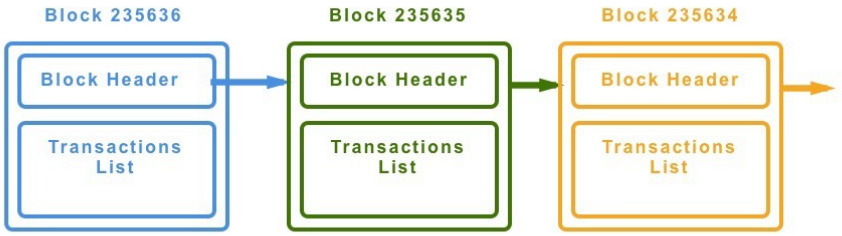
6.7.2020.

Sadržaj

- Tehnologija glavne raspodijeljene knjige
- Ethereum
- Sklopovlje
- Mreža i performance
  - Postavljanje mreže
  - Praćenje stanja (engl. *monitoring*)
- Zaključak

Tehnologija glavne raspodijeljene knjige

- Blockchain
- Algoritmi konsenzusa
  - Proof of Work
  - Proof of Stake
  - Proof of Authority



Ethereum

- Buterinov whitepaper iz 2013. godine
- Proof of Work (prijelaz na Proof of Stake)
- Geth i Parity implementacije programske podrške
- Pametni ugovori pisani u jeziku Solidity
  - Decentralizirane aplikacije
    - Cryptokitties

Sklopovlje

- Cubieboard2 - ARM
- Raspberry Pi 1 model B - ARM
- Raspberry Pi 3 model B - ARM
- Prijenosno računalo – Intel Pentium 64 bit
- Stolno računalo – AMD Phenom II X4 64 bit

Postavljanje mreže

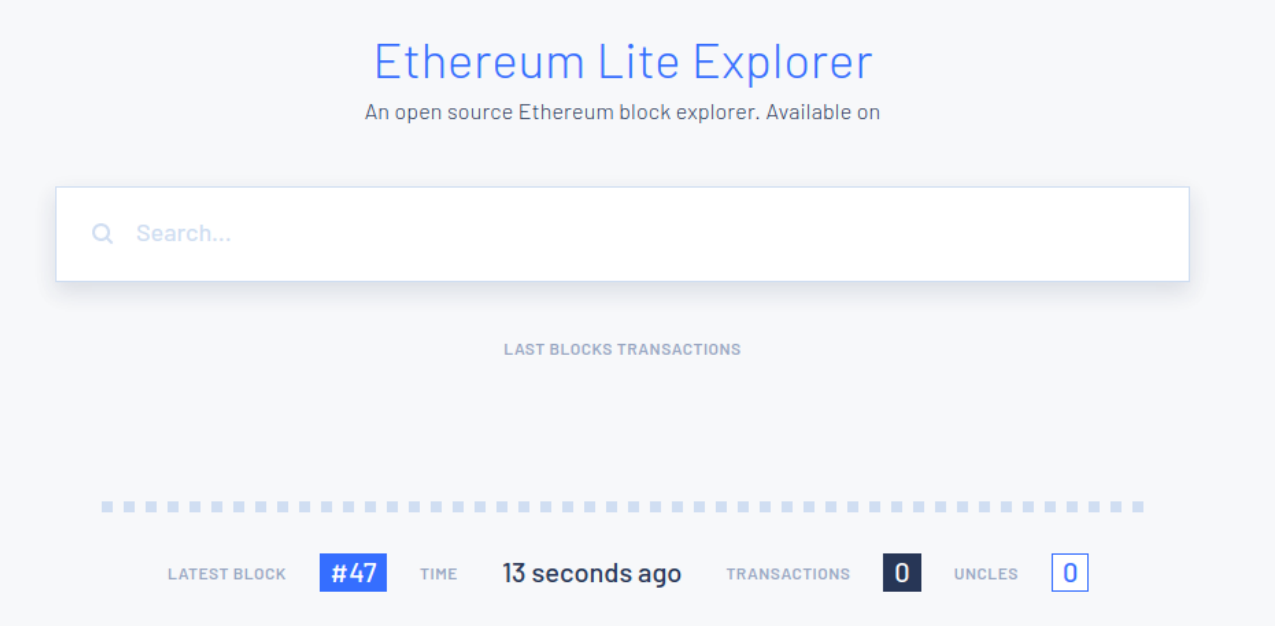
- Generiranje adresa i novčanika za svaki čvor
- Konfiguracija mreže i prvog bloka (genesis.json)
  - Inicijalizacija čvorova genesis.json datotekom
- Konfiguracija bootnodea
  - `$ bootnode -genkey boot.key`
- Pokretanje Geth procesa na svim čvorovima

Pokretanje Geth procesa

```
jakic007@jakic007-Aspire-E5-511G:~/Documents/FER/ZR/poa$ geth --datadir node4/ --syncmode 'full' --bootnodes 'enode://e5901c099c7894f23427f0d433f0edbfda01fd88e7788585dc3994a39f7e5e0f6185b96e9
63dd4071263a447ec10133725e470a2b830ecab9daffe29f66132d@192.168.1.13:0?discport=30310' --networkid 15316 --gasprice '1' -unlock '0xaD59dA52E58E82799bfB7cC360f49Eed872Bc586' --allow-insecure-un
ock --mine
INFO [05-19|20:43:06.675] Maximum peer count                       ETH=50 LES=0 total=50
INFO [05-19|20:43:06.676] Smartcard socket not found, disabling    err="stat /run/pcscd/pcscd.comm: no such file or directory"
WARN [05-19|20:43:06.680] The flag --gasprice is deprecated and will be removed in the future, please use --miner.gasprice
INFO [05-19|20:43:06.681] Starting peer-to-peer node               instance=Geth/v1.9.14-stable-6d74d1e5/linux-amd64/go1.14.2
INFO [05-19|20:43:06.682] Allocated trie memory caches             clean=256.00MiB dirty=256.00MiB
INFO [05-19|20:43:06.682] Allocated cache and file handles         database=/home/jakic007/Documents/FER/ZR/poa/node4/geth/chaindata cache=512.00MiB handles=524288
INFO [05-19|20:43:06.725] Opened ancient database                  database=/home/jakic007/Documents/FER/ZR/poa/node4/geth/chaindata/ancient
INFO [05-19|20:43:06.725] Initialised chain configuration          config="{ChainID: 15316 Homestead: 0 DAO: <nil> DAOSupport: false EIP150: 0 EIP155: 0 EIP158: 0 Byzantium: 0 Constantinople:
0 Petersburg: 0 Istanbul: 0, Muir Glacier: <nil>, Engine: clique}"
INFO [05-19|20:43:06.726] Initialising Ethereum protocol           versions="[65 64 63]" network=15316 dbversion=<nil>
WARN [05-19|20:43:06.726] Upgrade blockchain database version      from=<nil> to=7
INFO [05-19|20:43:06.727] Loaded most recent local header          number=0 hash="9bcbfc…dac475" td=1 age=19m39s
INFO [05-19|20:43:06.727] Loaded most recent local full block      number=0 hash="9bcbfc…dac475" td=1 age=19m39s
INFO [05-19|20:43:06.727] Loaded most recent local fast block      number=0 hash="9bcbfc…dac475" td=1 age=19m39s
INFO [05-19|20:43:06.728] Regenerated local transaction journal    transactions=0 accounts=0
INFO [05-19|20:43:06.730] Stored checkpoint snapshot to disk       number=0 hash="9bcbfc…dac475"
INFO [05-19|20:43:06.747] New local node record                    seq=1 id=f9033243d81eeee3 ip=127.0.0.1 udp=30303 tcp=30303
INFO [05-19|20:43:06.748] Started P2P networking                   self=enode://db68f87adb1d8267bbe403be0c11cd2430d4a9b98c1a635b49591aaa3bae51abcdf4663774ef283ea1feb6209e8ec2a68b09936d6ae633f4
26be28b117636d6d@127.0.0.1:30303
INFO [05-19|20:43:06.754] IPC endpoint opened                      url=/home/jakic007/Documents/FER/ZR/poa/node4/geth.ipc
Unlocking account 0xaD59dA52E58E82799bfB7cC360f49Eed872Bc586 | Attempt 1/3
Password:
INFO [05-19|20:43:11.093] Unlocked account                         address=0xaD59dA52E58E82799bfB7cC360f49Eed872Bc586
INFO [05-19|20:43:11.094] Transaction pool price threshold updated price=1
INFO [05-19|20:43:11.094] Transaction pool price threshold updated price=1
INFO [05-19|20:43:11.094] Etherbase automatically configured       address=0xaD59dA52E58E82799bfB7cC360f49Eed872Bc586
INFO [05-19|20:43:11.094] Commit new mining work                   number=1 sealhash="f06f0a…27fd57" uncles=0 txs=0 gas=0 fees=0 elapsed="194.689µs"
INFO [05-19|20:43:11.099] Successfully sealed new block            number=1 sealhash="f06f0a…27fd57" hash="a1ed9c…64c5e7" elapsed=4.587ms
INFO [05-19|20:43:11.099] ↖ mined potential block                   number=1 hash="a1ed9c…64c5e7"
INFO [05-19|20:43:11.100] Commit new mining work                   number=2 sealhash="43a2f4…ab53f7" uncles=0 txs=0 gas=0 fees=0 elapsed=1.327ms
INFO [05-19|20:43:11.101] Signed recently, must wait for others
INFO [05-19|20:43:17.310] Looking for peers                        peercount=0 tried=0 static=0
```

Praćenje stanja

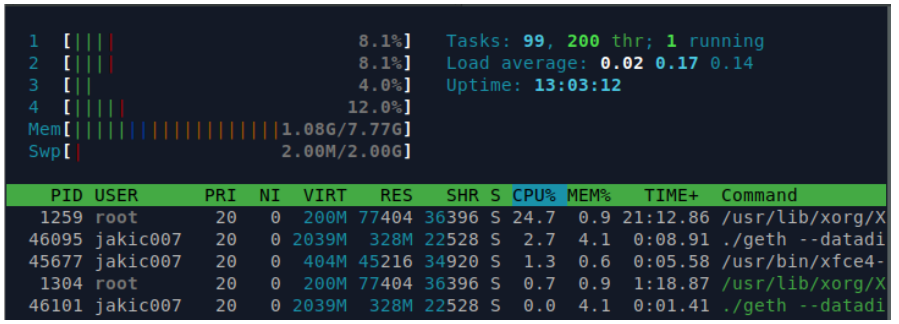
- Pretražitelji blokova (engl. *block explorer*)
- Ethstats za pregled performanci čvora
- Htop



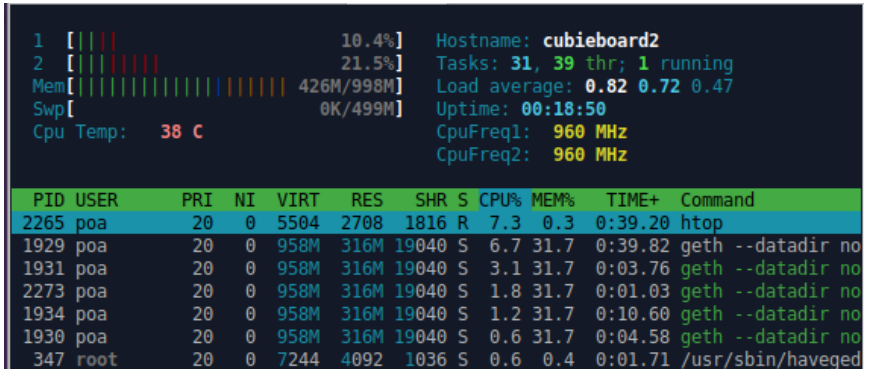
Ethstats pregled

htop ispis

- Osobno računalo



- Cubieboard2



Zaključak

- Vrlo dostupna dokumentacija
- Proof of Authority algoritam ima vrlo niske zahtjeve na sklopovlje
- Potrebno predznanje i razumijevanje arhitekture mreže
- Količina podataka konstantno raste i zahtjeva dovoljno slobodne memorije za pohranu na čvorovima