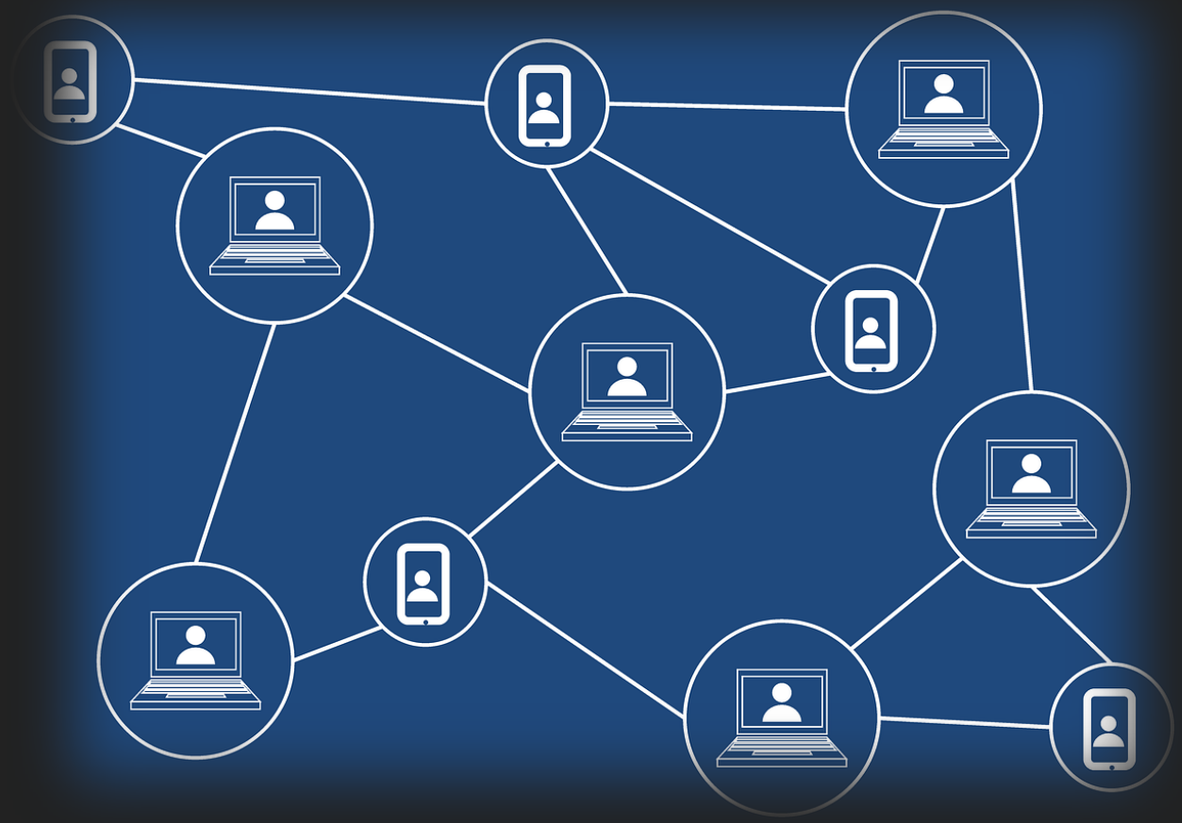


AUTOR: BERNARD CRNKOVIĆ

MENTOR: PROF. DR. SC. MARIN GOLUB

AK. GOD. 2021.

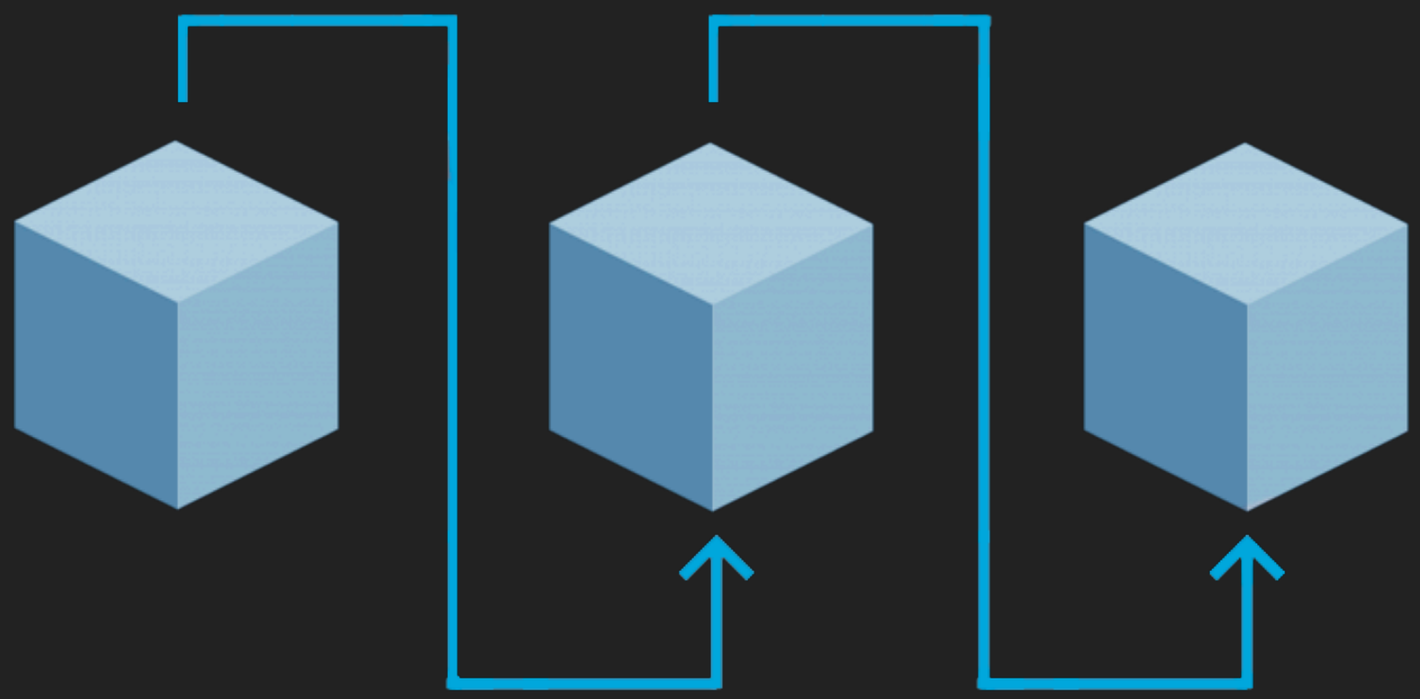
ZAVRŠNI RAD: LANAC STRANICA I DISTRIBUIRANO SUGLASJE U SUSTAVIMA ELEKTRONIČKOG NOVCA

UVOD

- centraliziranost bankarskih sustava
- ranjivost - *single point of failure*
- povjerenje u centralni autoritet
- loša normiranost
- zastarjeli protokoli (SWIFTNet)

DEFINICIJA LANCA STRANICA

- struktura podataka s elementima ulančanim sažetcima
- elementi su liste tvrdnji - transakcija



IMPLEMENTACIJE

- na stranice zapisujemo digitalno potpisane transakcije
- preslikavanje javnog ključa u adresu novčanika
- mreža prihvaća samo ispravne tvrdnje
- traženje sažetka s N nul-bitova - *difficulty*
- rudari stvaraju nove stranice - popisi ispravnih transakcija
- naknada rudaru - incentiva

METODE POSTIZANJA SUGLASJA U MREŽAMA BEZ POVJERENJA

- dokaz rada
  - kriptovaluta Bitcoin
  - problemi: specijalizirani hardver → centralizacija
- dokaz uloga
  - kriptovaluta Cardano
  - problemi: potrebna 2/3 iskrenih/funkcionalnih čvorova zbog problema bizantskih generala

ROBUSNOST PROTOKOLA

- anonimnost - *Gossip* protokol Bitcoin mreže
  - otežani usmjereni napadi na žrtvu
- vjerojatnost uspjeha napada proporcionalna uloženoj količini računalne snage
- otpornost na CPU manjinu malicioznih aktora (< 50%)

PROBLEMI DOKAZA RADA

- niska propusnost
- neekonomičnost
- podložnost centralizaciji procesorske snage

DOKAZ ULOGA

- vjerojatnost da čvoru bude dodjeljena uloga rudara proporcionalna je pologu
- *Ouroboros* protokol kriptovalute Cardano
- dijeljenjem lanca na više *shardova* s manjim komitetima rudara
- kraće vrijeme potvrde
- povremena sinkronizacija sa ostalim shardovima

PROGRAMSKA PODRŠKA

- Logika čvora

python™

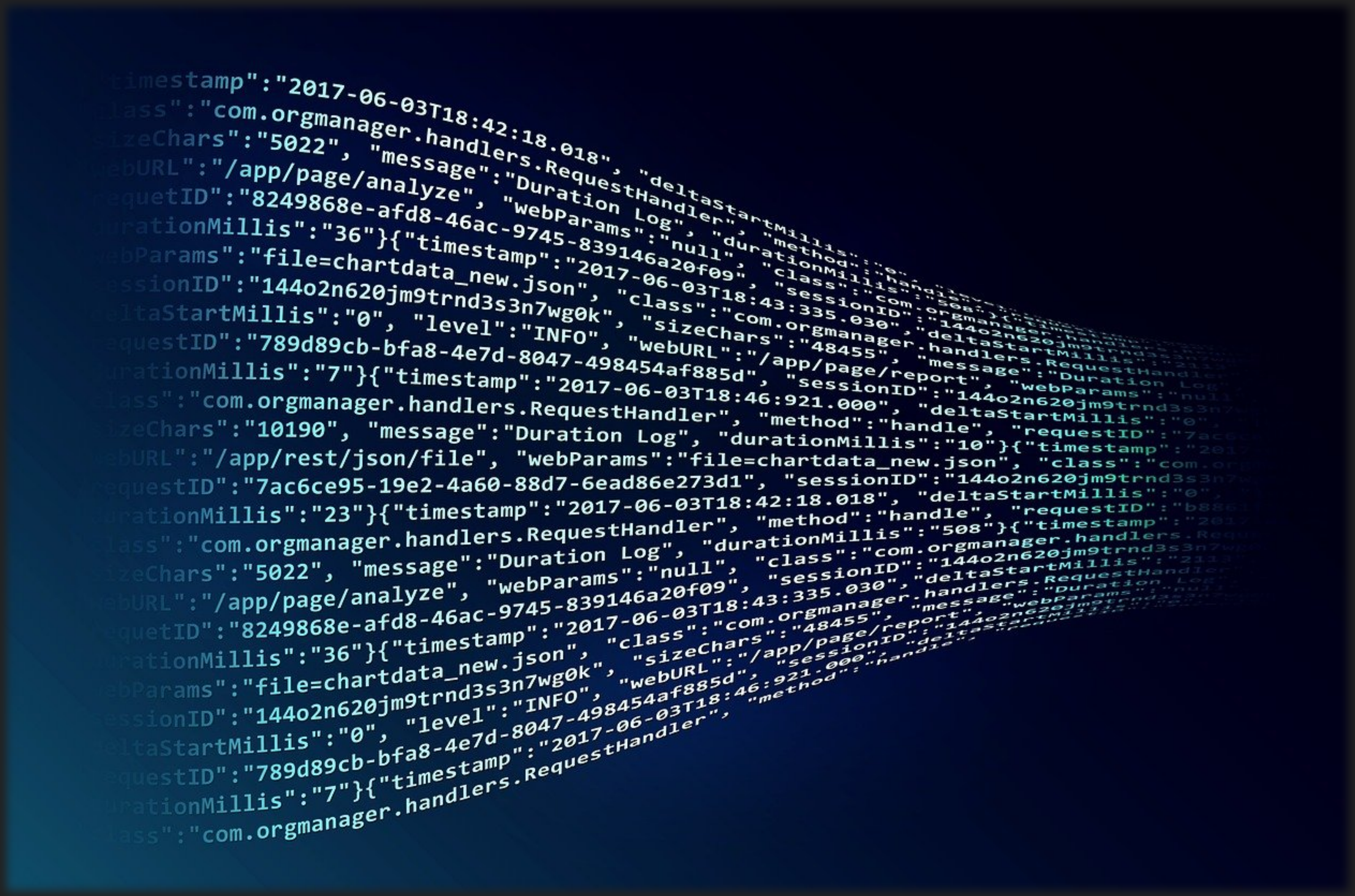
Flask

web development,
one drop at a time

- Web sučelje

POVEZIVANJE BACKENDA I FRONTENDA

- klasično REST sučelje bazirano na HTTP
- JSON za format objekta prijenosa podataka



SIMULACIJA

ZAKLJUČAK

- ubrzani razvoj tehnologija lanca stranica
- potaknuo brojna znanstvena istraživanja u području distribuiranog računarstva i računalnoj sigurnosti
- korak prema transparentnom sustavu novca

LITERATURA

- Radovi:
  - Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. U OSDI, svezak 99, stranice 173–186, 1999.
  - Leslie Lamport, Robert Shostak, i Marshall Pease. The byzantine generals pro- blem. ACM Transactions on Programming Languages and Systems
  - Aggelos Kiayias, Alexander Russell, Bernardo David, i Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol
  - Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system
  - Canhui Wang, Xiaowen Chu, i Yang Qin. Measurement and analysis of the bitcoin networks: A view from mining pools
  - Central authority – Wikipedia https://en.wikipedia.org/w/index.php?title=Central_Authority&oldid=969028445
  - Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger
- Prezentacija:
  - uzorak: Keynote template
  - slike: https://pixabay.com

HVALA VAM NA PAŽNJI!

Q&A