



Konferencija Srce DEI

Agentsko modeliranje konsenzusa u DLT sustavima

Matija Piškorec

Institut Ruđer Bošković

Srce DEI 2026



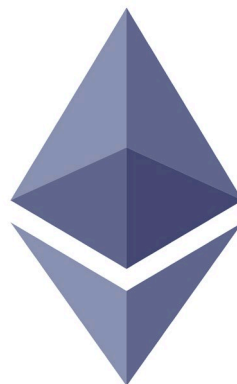


DLT sustavi

DLT (eng. Distributed Ledger Technologies) – Raspodijeljene glavne knjige, digitalni zapis transakcija bez centralnog pohranjivanja.



Bitcoin



Ethereum



Solana



DLT sustavi – čemu služe?

Bitcoin protokol je prva uspješna implementacija DLT sustava (2008.) – digitalnog zapisa transakcija bez centralne pohrane, koji koristi konsenzus protokol kako bi osigurao da svi sudionici imaju identične kopije transakcija.

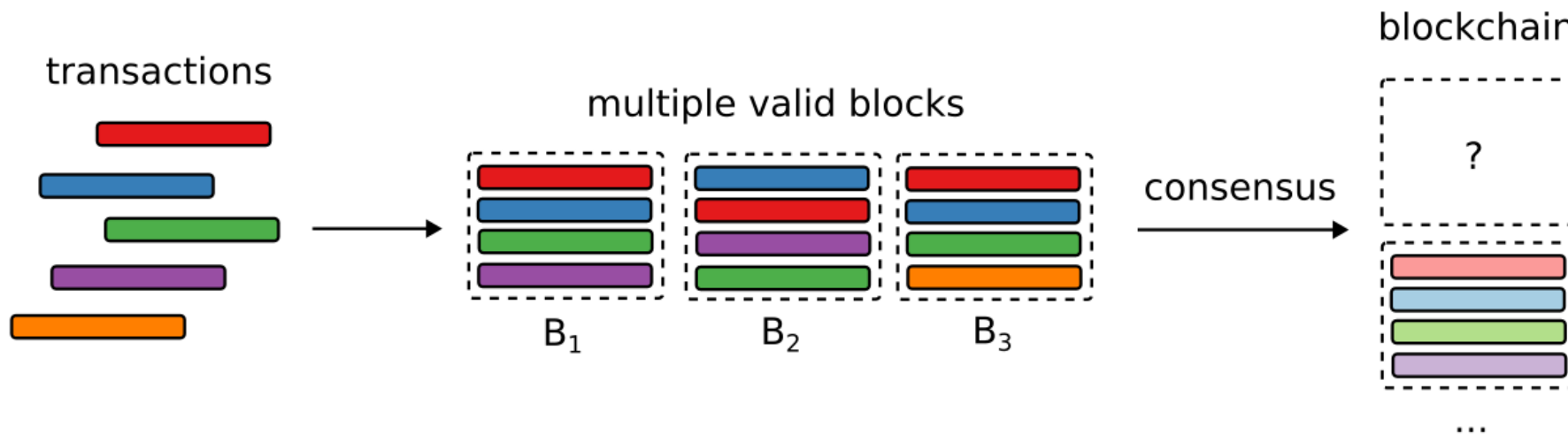
“electronic payment system based on cryptographic proof instead of trust, allowing two willing parties to transact directly with each other without the need for a trusted third party”



„Bitcoin: A Peer-to-Peer Electronic Cash System” (2008) <https://bitcoin.org/en/bitcoin-paper>



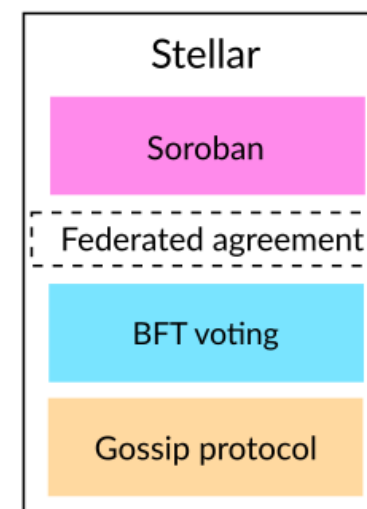
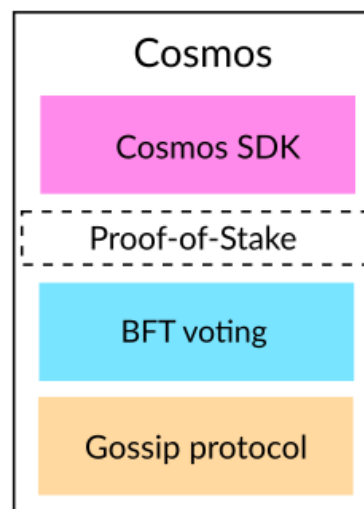
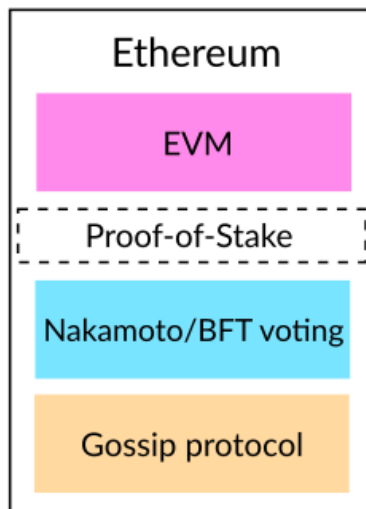
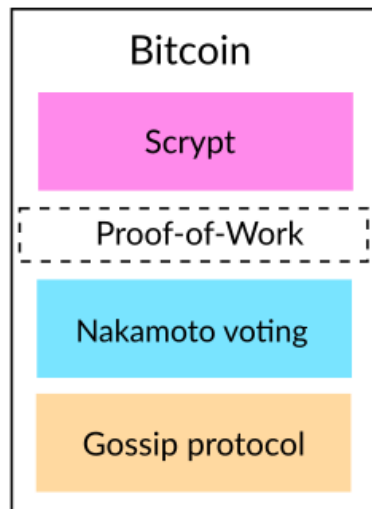
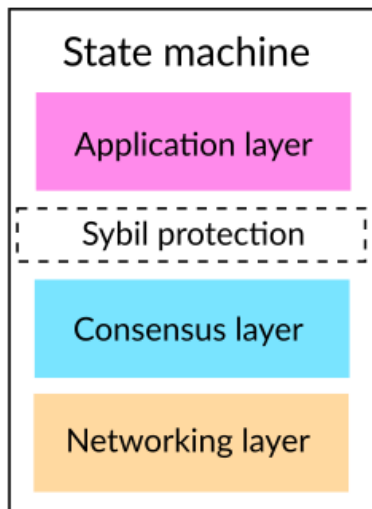
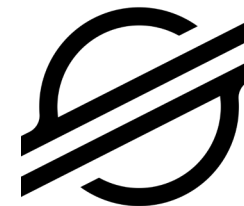
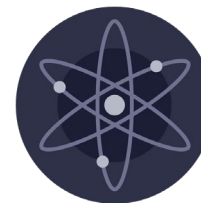
Konsenzus u DLT sustavima



- **Konsenzus** – Protokol koji osigurava da svi sudionici imaju identične kopije transakcija u **identičnom redoslijedu**.
- **Blockchain** (hrv. ulančani blokovi) je posebno pogodna struktura podataka za DLT sustave jer su blokovi kriptografski povezani i ne mogu se mijenjati bez da se promijene svi ostali blokovi!



Arhitektura DLT sustava





Konsenzus protokoli u DLT sustavima

Svaki konsenzus protokol u DLT sustavima sastoji se od dvije komponente:

- **Pravila glasanja** – Kojima sudionici odlučuju koje transakcije prihvatiti i kojim redoslijedom.
 - *Nakamoto glasanje* – Prihvati najduži validni slijed transakcija.
 - *BFT* (eng. Byzantine Fault Tolerant) *glasanje* – Saznaj kako glasaju sudinici kojima vjeruješ i kroz višestruke runde glasanja prihvati isti slijed transakcija kao i oni.
- **Sybilska zaštita** – Koja osigurava da sudionici ne mogu nepravedno dominirati glasanjem, u svrhu glasanja moraju predočiti nešto se ne može lako lažirati.
 - Proof-of-Work (PoW) – računalna snaga (hashpower)
 - Proof-of-Stake (PoS) – udio u nativnoj valuti koja se bilježi u transakcijama (npr. Ether)

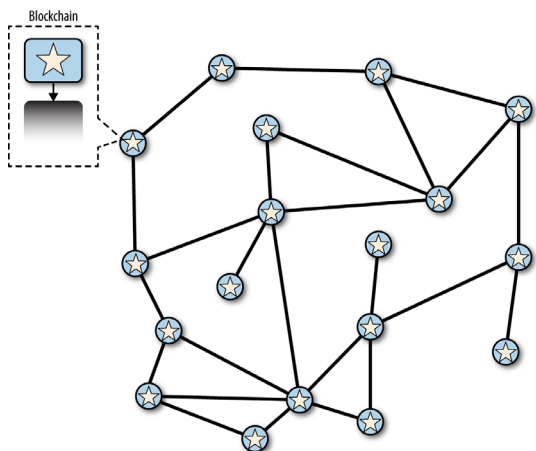


Konsenzus protokoli u DLT sustavima

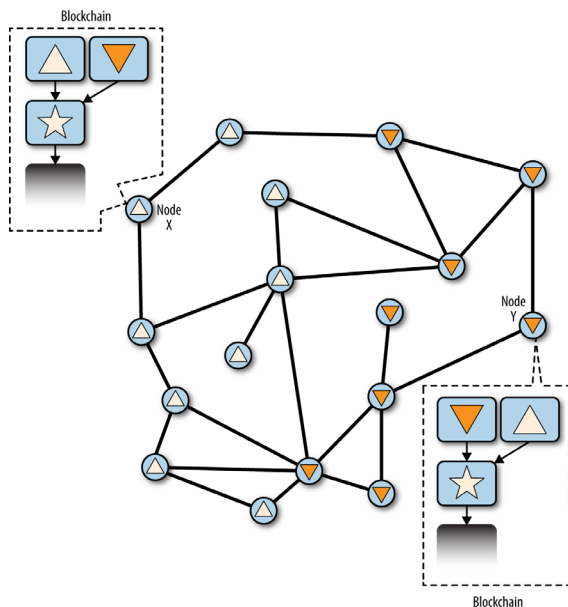
Voting rules → Sybil protection ↓	Nakamoto-style (longest chain and variants)	BFT-style (voting-based consensus with quorums)
Proof-of-Work	Bitcoin PoW Ethereum (before 2022)	
Proof-of-Stake	Ouroboros Ethereum (after 2022) [†]	Algorand Tendermint Solana Polkadot
Federated Byzantine Agreement		XRP Ledger Stellar Consensus Protocol SCP



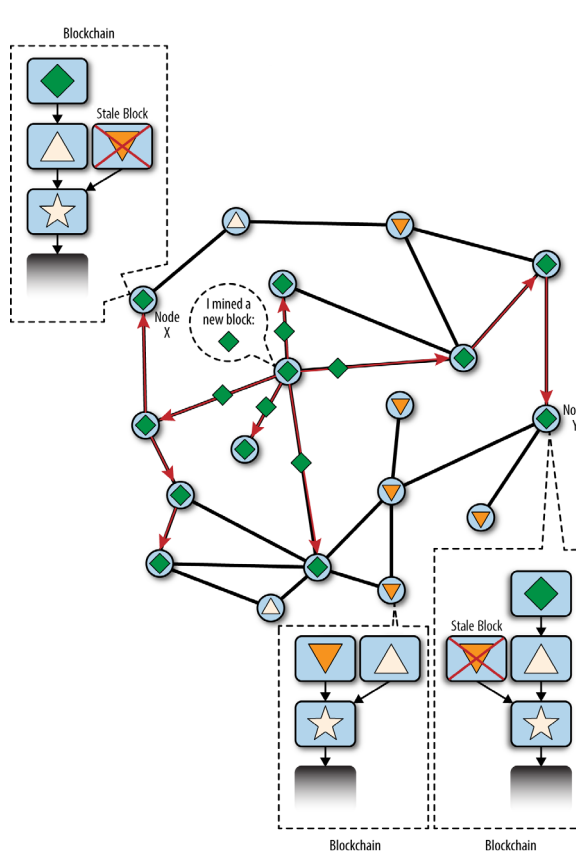
Konsenzus u Proof-of-Work protokolu (Bitcoin)



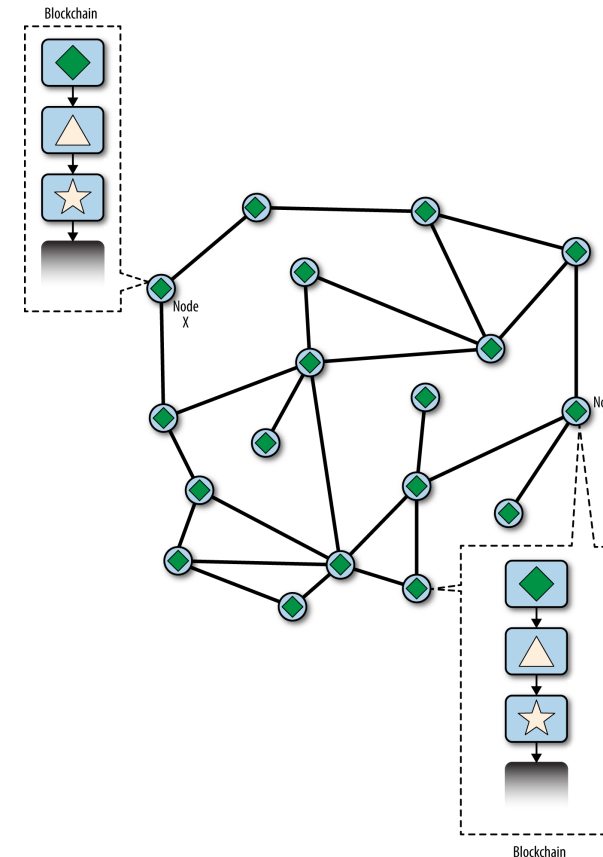
Svi sudionici su u konsenzusu



Konsenzus je privremeno narušen – istovremeno se pojavljuju dva validna bloka, blockchain se račva (fork)



Sudionici čekaju na nove blokove i prihvaćaju najduži validni lanac blokova (Nakamoto glasanje)

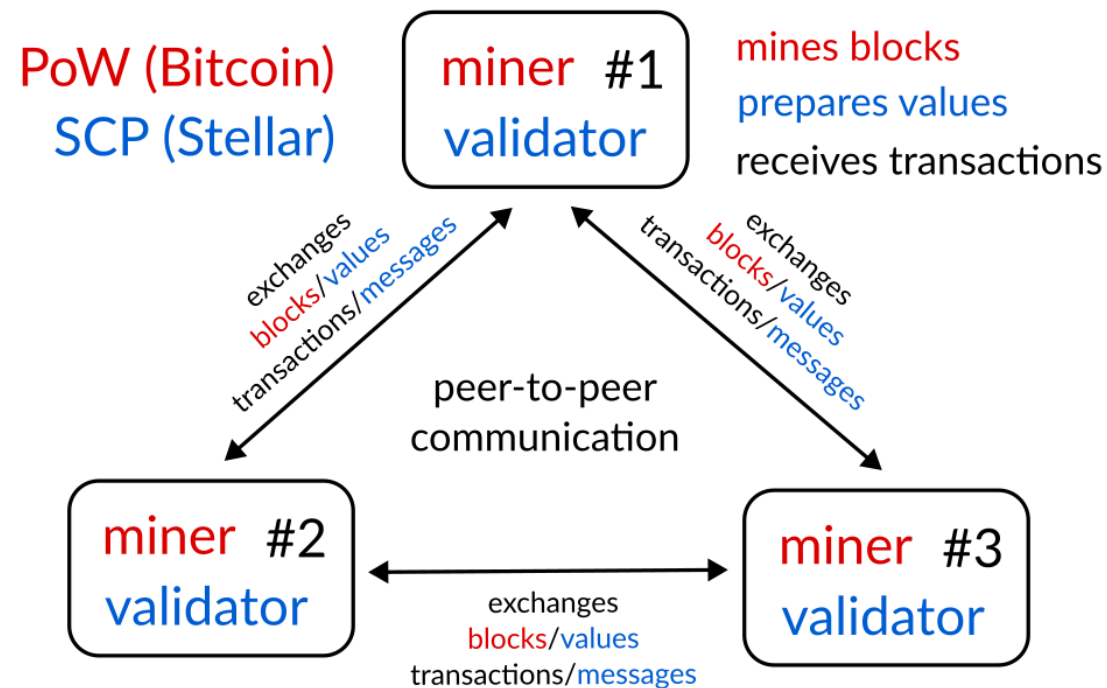


Konsenzus je ponovno uspostavljen!

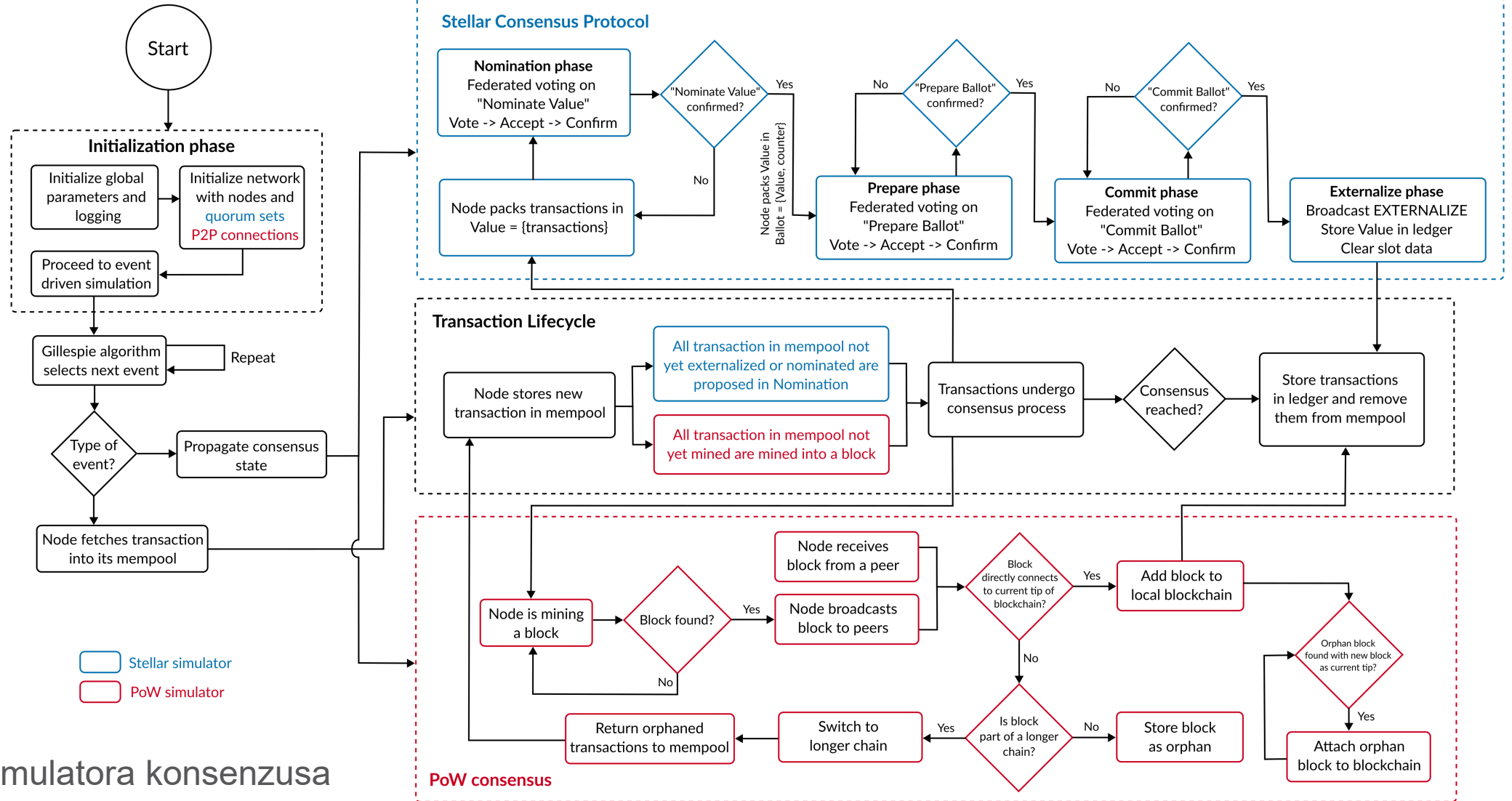


Agentsko modeliranje DLT konsenzusa

- Koristimo **Gillespijev algoritam** za simuliranje događaja u **agentskom modelu** konsenzusa u DLT sustavima.
- Gillespijev algoritam pretpostavlja da su događaji međusobno nezavisni i da njihov vremenski slijed prati eksponencijalnu distribuciju.
- Primjer događaju u simulatoru konsenzusa:
 - Dohvaćanje transakcije (PoW i SCP)
 - Komunikacija (PoW i SCP)
 - Rudarenje bloka transakcija (PoW)



Daniel T. Gillespie. "A general method for numerically simulating the stochastic time evolution of coupled chemical reactions". Journal of computational physics, 22(4):403–434, 1976.



Arhitektura simulatora konsenzusa

<https://github.com/matijapiskorec/stellar-simulator>



Stvaranje transakcija u simulatoru

EXECUTION TIME - CLASS - VERBOSITY LEVEL - DESCRIPTION (where time is a simulation time!)

720.00 - TRANSACTION - INFO - Created transaction with hash d19e1df5 and time 0

720.00 - MEMPOOL - INFO - Transaction [Transaction d19e1df5 time = 0.0000] mined to the mempool!

...

720.00 - SIMULATOR - INFO - Handling event retrieve_transaction_from_mempool at simulation time = 0.030

721.00 - MEMPOOL - INFO - Transaction [Transaction d19e1df5 time = 0.0000] retrieved from the mempool!

721.00 - NODE - INFO - Node 1 retrieved [Transaction d19e1df5 time = 0.0000] from mempool.

721.00 - LEDGER - INFO - Node 1: transaction [Transaction d19e1df5 time = 0.0000] added!

...



Razmijena poruka u simulatoru

EXECUTION TIME - CLASS - VERBOSITY LEVEL - DESCRIPTION (where time is a simulation time!)

721.00 - MESSAGE - INFO - Created SCPNominate message,

data = [SCPNominate message,

data = {'_message_id': '0b5228d9b3',

'_broadcasted': True,

'_voted': [[Value, hash = 8329928684640308105,

state = State.init,

transactions = [[Transaction d19e1df5 time = 0.0000]]],

'_accepted': []]

721.00 - STORAGE - INFO - Node 1: added message [SCPNominate message, ...]

721.00 - NODE - INFO - Node 1 appended SCPNominate message to its storage , message = [...]



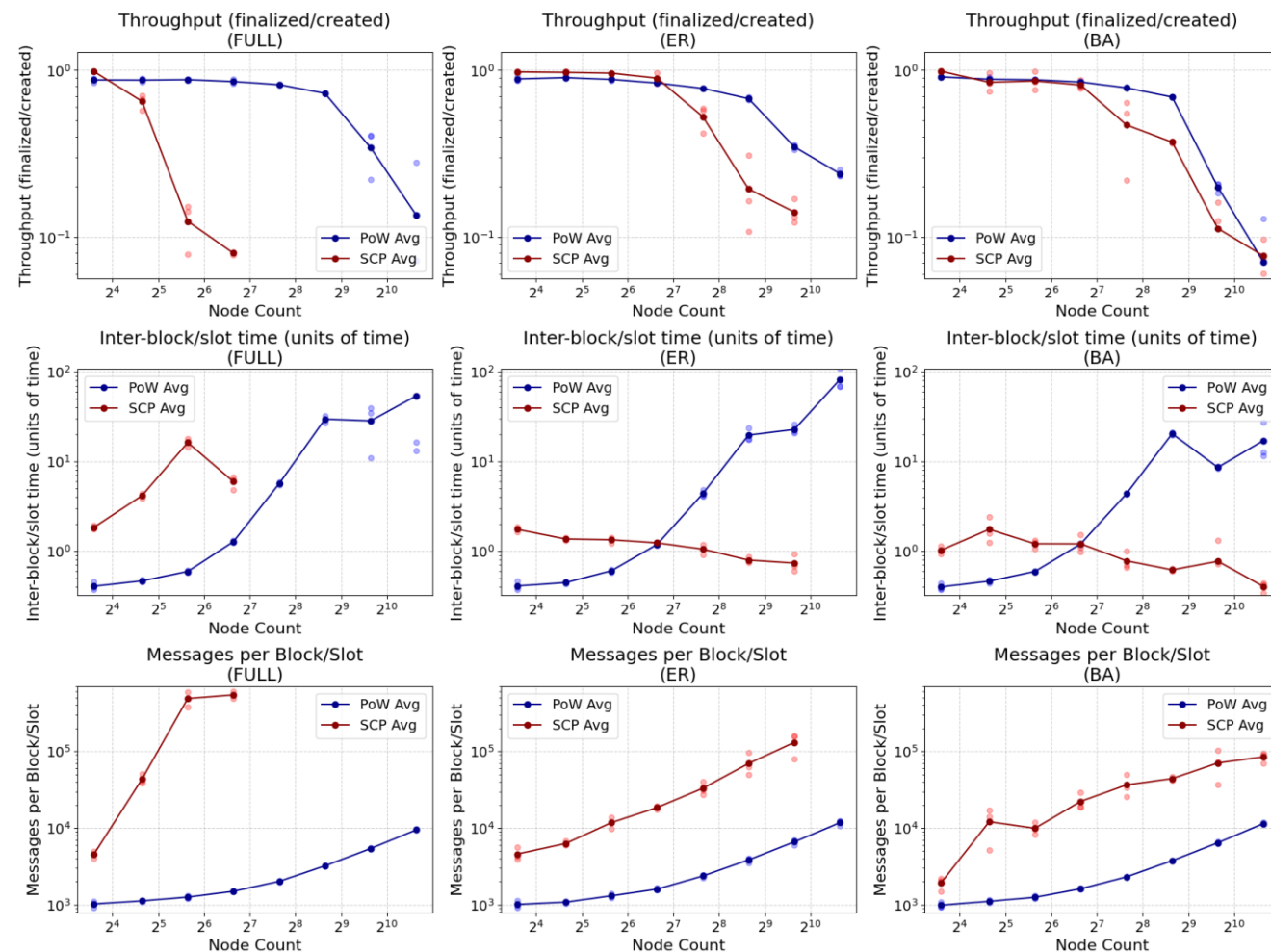
Eksperimenti

Eksperimenti su provedeni na HPC infrastrukturi Sveučilišta u Zurichu.

Simulacije su međusobno nezavisne pa je paralelizacija na više nezavisnih HPC čvorova jednostavna.

Rezultati:

- **Skalabilnost:** PoW može obraditi više transakcija u jedinici vremena od SCP-a.
- **Decentraliziranost:** U PoW-u može sudjelovati više sudionika nego u SCP-u.
- PoW ima razmijenjuje manje poruka od SCP-a.





Istraživačka pitanja

Koje su performanse različitih DLT konsenzus protokola s obzirom na:

- **Sigurnost** – garancije da će konsenzus uvijek uspjeti bez obzira na uvjete
- **Skalabilnost** – mogućnost obrade što većeg broja transakcija u jedinici vremena
- **Decentralizaciju** – najveći mogući broj sudionika u konsenzusu

Smatra se da je nemoguće zadovoljiti sva tri uvjeta – **blockchain trilema!**

Vitalik Buterin, "The Blockchain Trilemma", <https://vitalik.ca/general/2021/06/17/trilemma.html>



Tražimo doktoranda!

Projekt: „Autonomni agenti u protokolima raspodijeljenih glavnih knjiga“

Lokacija: Institutu Ruđer Bošković, Zavod za računarstvo i podatkovnu znanost

Radno mjesto: asistent (doktorand)

Suradnja: dr. sc. Matija Piškorec, dr. sc. Damir Korenčić

Početak: (očekivano) kraj 2026.

Tražimo: magistre računarstva, fizike, matematike i ostalih tehničkih i prirodnih smjerova koji žele raditi doktorsko istraživanje na temama iz umjetne inteligencije i DLT sustava

Kontakt: matija.piskorec@irb.hr



Hvala vam na pažnji!

Matija.piskorec@irb.hr



Ovo djelo je dano na korištenje pod licencom Creative Commons *Imenovanje* 4.0 međunarodna.

Srce politikom otvorenog pristupa široj javnosti osigurava dostupnost i korištenje svih rezultata rada Srca, a prvenstveno obrazovnih i stručnih informacija i sadržaja nastalih djelovanjem i radom Srca.

www.srce.unizg.hr

creativecommons.org/licenses/by/4.0/deed

www.srce.unizg.hr/otvoreni-pristup

