

# Testiranje zmogljivosti omrežij blokovnih verig z orodjem Hyperledger Caliper

Leon Ciglar<sup>1</sup>, Matevž Pustišek<sup>2</sup>

<sup>1,2</sup>Fakulteta za elektrotehniko, Univerza v Ljubljani  
E-pošta: <sup>1</sup>lc3882@student.uni-lj.si, <sup>2</sup>matevz.pustisek@fe.uni-lj.si

## Blockchain network performance testing with the Hyperledger Caliper tool

**Abstract.** *Distributed ledger technologies, such as blockchain, have emerged as crucial innovations for ensuring secure, transparent, and decentralized data recording and exchange. However, challenges related to scalability and performance hinder their widespread implementation and further development. This research focuses on the analysis of blockchain network performance, the identification of key performance parameters and the evaluation of a dedicated tool called Hyperledger Caliper. Within this study, we examine the response of a local Ethereum network under increased load to determine its limitations. Moreover, our research introduces an indicator for real-time diagnostics of blockchain networks that can be applied to any public or private networks without significant cost or impact on the network, capable of efficiently detecting load spikes in blockchain networks with minimal latency.*

## 1 Uvod

V zadnjem desetletju je tehnologija razpršene evidence (angl. Distributed ledger technology, DLT) doživela izjemen vzpon in postala pomembna inovacija za varno in transparentno upravljanje podatkov ter izvajanje transakcij. DLT uvaja nov pristop k zapisovanju, izmenjavi in sinhronizaciji podatkov, z uporabo številnih vozlišč (angl. Node), ki brez osrednje avtoritete, s pomočjo konsenznega mehanizma neodvisno vzdržujejo in posodablajo skupno zbirko podatkov [1]. Ena izmed najbolj priljubljenih implementacij DLT-ja so omrežja blokovnih verig (angl. Blockchain). Gre za seznam podatkovnih blokov, ustvarjen s soglasjem med enakovrednimi uporabniki. V blokih so zapisane transakcije (Tx), vsak od blokov pa je označen s časovnim žigom ter se s pomočjo kriptografskih odtisov (angl. Hash) nanaša na prejšnji blok, kar zagotavlja nespremenljiv zapis vseh transakcij v verigi, začevši s prvim blokom, znanim tudi kot blok geneze. V kontekstu veriženja blokov velja, da pri transakcijah, ki so uvrščene v pomnilniški sklad, ne prihaja do izgub in bodo prej ali slej uvrščene v blok, zato je omrežje blokovnih verig s tega vidika brezizgubno. Za razliko od tradicionalnih centraliziranih tehnologij ima tehnologija veriženja blokov nekaj pomembnih prednosti, kot so decentraliziranost, nespremenljivost podatkov, manjša verjetnost napak, večja transparentnost in zaupanja vredna obdelava

transakcij s t.i. pametnimi pogodbami (angl. Smart contract), ki so podlaga za decentralizirane aplikacije.

Pri raziskovanju in uporabi tehnologij razpršene evidence je bistvenega pomena za njihovo učinkovitost in praktično uporabnost njihova zmogljivost. Zaradi omejitve zmogljivosti uporaba omrežij blokovnih verig predstavlja izziv, še posebej v sistemih, ki zahtevajo visoke hitrosti, kot sta na primer obdelava spletnih transakcij (angl. Online transaction processing) in plačilnih sistemih v realnem času [2]. Kajti v nasprotju z obstoječimi centraliziranimi plačilnimi sistemi, kot sta VisaNet ali MasterCard, ki lahko obdelajo tisoče transakcij na sekundo, javno omrežje Ethereum omogoča zgolj 12-15 transakcij na sekundo. Prav zato je razumevanje in analiziranje obnašanja omrežij blokovnih verig v različnih okoljih in pri različnih obremenitvah ključno, za nadaljnji razvoj, praktično uporabnost, pridobitev zaupanja in sprejetja s strani poslovnega in širšega uporabniškega občinstva. Tu pa se pojavlja ključno vprašanje: kako meriti in ocenjevati zmogljivost teh omrežij?

V ta namen smo se lotili raziskave, skozi katero smo analizirali zmogljivost omrežij blokovnih verig, raziskali kaj so ključni parametri zmogljivosti in preizkusili namensko orodje Hyperledger Caliper. Analizirali smo odziv emuliranega Ethereum omrežja na povečano obremenitev in poiskali praktično rešitev - indikator za zaznavanje povečanih obremenitev v omrežjih blokovnih verig, kar lahko koristi raziskovalcem, razvijalcem in uporabnikom omrežij blokovnih verig.

## 2 Zmogljivost omrežij blokovnih verig

Na zmogljivosti omrežij blokovnih verig vpliva več dejavnikov, eden ključnih je sam koncept omrežja in njegova velikost. Gre za omrežni model enakovrednih udeležencev (angl. Peer-to-peer, P2P) zato je jasno, da bo velikost oziroma število vozlišč vplivalo na propagacijski čas - to je čas, ki je potreben, da se sporočilo ali informacija prenese od enega vozlišča do vseh drugih, ciljnih vozlišč v omrežju. Potrebno je poudariti, da večjega števila vozlišč v omrežjih DLT ne uporabimo z namenom izboljšanja zmogljivost omrežja, pač pa je glavni namen velikega števila vozlišč decentraliziranost, večja stabilnost, odpornost na napake in večje zaupanje v podatke, ki jih shranimo v razpršeno evidenco.

Drug pomemben dejavnik, ki vpliva na zmogljivost omrežij blokovnih verig, je tehnologija, ki se uporablja za gradnjo teh omrežij. Na voljo je več platform in

protokolov za izvedbo omrežij DLT, kot na primer Ethereum, Hyperledger Fabric, IOTA in mnoge druge. Zaradi različne strukture, potrjevanja in dodajanja transakcij v nespremenljive gruče imamo lahko v različnih omrežjih povsem drugačne poglede na potrditev (angl. Confirmation) in končnost (angl. Finality) transakcij ter s tem na zmogljivost omrežij. Še bolj zanimivo pa je, da lahko že z isto tehnologijo dosežemo popolnoma različne zmogljivosti in značilnosti, odvisno od načina implementacije in konfiguracije. Poleg tega v splošnem na zakasnitve v omrežju vpliva čas generiranja in validacije transakcij, čas ustvarjanja in velikost bloka ter čas za doseganje zadostne mere dokončnosti [1].

## 2.1 Vrednotenje zmogljivosti

Najpogosteje zmogljivost sistema veriženja blokov ocenjujemo v dveh dimenzijah, in sicer: latenci (angl. Latency), ki meri, kako hitro je posamezna transakcija potrjena, in prepustnosti (angl. Throughput), ki meri, koliko transakcij lahko sistem obdela v določenem časovnem obdobju. Največkrat prepustnost merimo v sekundnih intervalih, torej: koliko transakcij lahko sistem obdela v sekundi (angl. Transactions per second, TPS) [3]. Kljub temu da imamo le dva ključna parametra, analiza zmogljivosti ni tako preprosta, saj se pri merjenju latence in prepustnosti pojavi veliko dilem, na primer: kdaj začnemo meriti latenco, ko kliknemo "pošlji" ali, ko transakcija pride v pomnilniški sklad (angl. Mempool)? In kdaj ustavimo štoparico: ko je transakcija dodana v blok ali ko je blok potrjen z enim nadaljnjim blokom ali morda dvanajstimi? Poleg tega zaenkrat še ne obstajajo standardi, ki bi definirali parametre in način vrednotenja [4]. Zato so orodja, kot je Hyperledger Caliper lahko dobra pomoč pri sistematični analizi omrežij.

## 3 Analiza z orodjem Hyperledger Caliper

Hyperledger Caliper je odprtokodno orodje, predstavljeno leta 2018 v sklopu Hyperledger fundacije. Orodje je posebej zasnovano za merjenje zmogljivosti decentraliziranih omrežij blokovnih verig in omogoča analizo treh metrik analize: prepustnost transakcij/branj, zakasnitev transakcij/branj in porabo virov (procesor, pomnilnik, omrežni I/O itd.). Podpira več različnih omrežij in sicer Hyperledger Burrow, Ethereum, Hyperledger Fabric, FISCO BCOS, Hyperledger Iroha ter Hyperledger Sawtooth [5].

### 3.1 Potek analize

V sklopu raziskave smo se osredotočili na analizo emuliranega Ethereum omrežja, ki smo ga vzpostavili s pomočjo orodja Ganache. Je del razvijalskega okvirja Truffle suite in seta orodij, ki uporablja virtualni stroj Ethereum (angl. Ethereum Virtual Machine, EVM). Prvi del analize je zajemal obremenitveni test, kjer smo

emulirano omrežje (Tabela 1) obremenili do točke zasičenja in spremljali zakasnitve ter prepustnost.

Tabela 1. Nastavitve emuliranega Ethereum omrežja pri obremenitvenem testu

Parameter	Vrednost
Čas kreiranja bloka	12 s
Velikost bloka	100 Tx
Teoretična maksimalna prepustnost	8,33 TPS
Čas trajanja Caliper testa pri posamezni obremenitvi	100x čas kreiranja bloka

V sklopu drugega dela analize smo z enim testnim okoljem Caliper postopno obremenjevali omrežje (Tabela 2). Z drugim okoljem Caliper smo pošiljali posamezne merilne transakcije (angl. Ping) in saj smo želeli, s čim manjšim posegom v omrežje ugotoviti, ali prihaja do povečane obremenitve. Merilne transakcije smo pošiljali na 3, 5 oziroma 10 blokov.

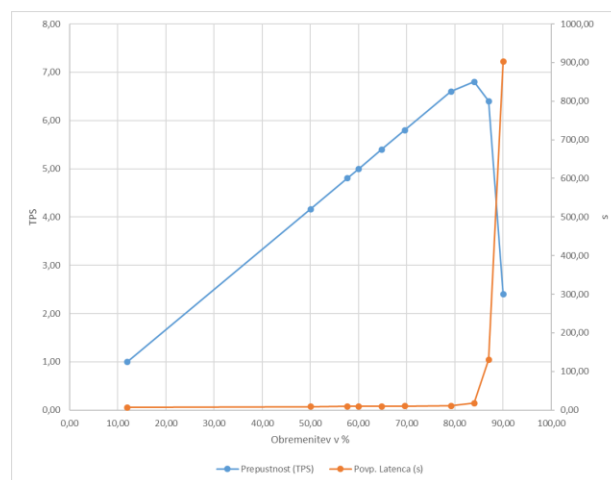
Tabela 2. Nastavitve emuliranega Ethereum omrežja pri sondiranju

Parameter	Vrednost
Čas kreiranja bloka	5 s
Velikost bloka	100 Tx
Teoretična maksimalna prepustnost	20 TPS
Čas trajanja Caliper testa pri posamezni obremenitvi	40x čas kreiranja bloka

## 4 Rezultati

### 4.1 Obremenitveni test

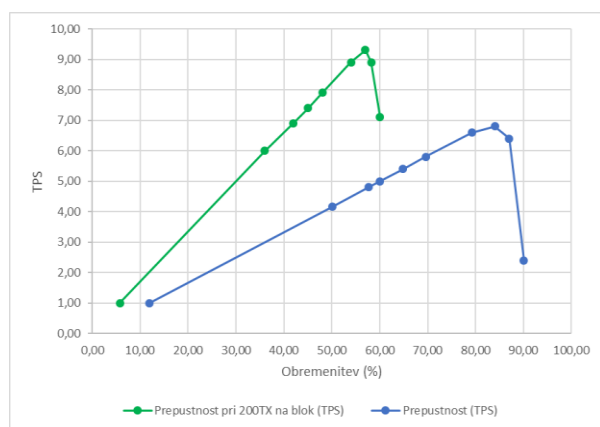
Rezultati meritve, pridobljeni iz poročila, ki ga generira Caliper, so prikazani na Slika 1, kjer je z modro označena prepustnost v TPS, z oranžno pa latenca v sekundah, oboje v odvisnosti od obremenitve omrežja v odstotkih.



Slika 1. Obremenitveni test emuliranega Ethereum omrežja.

Opazimo, da je omrežje blokovnih verig vse transakcije uspešno zapisalo v blok – nobena ni bila izgubljena. S povečevanjem obremenitve se latence minimalno povečujejo, do točke, ko pride v omrežju do prevelike obremenitve in se latenca eksponentno povečuje. To se je v predstavljenem primeru zgodilo pri približno 90 % obremenitvi, ko smo pošiljali s hitrostjo 7,5 TPS. Razlog smo interpretirali kot sistemsko omejitev, povezano z lokalnim okoljem oziroma razpoložljivo procesorsko močjo.

Zato smo meritev ponovili še za 2x večjo velikost bloka in 2x hitreje pošiljali transakcije. Vsi ostali parametri so ostali nespremenjeni. Pričakovali bi, da bo naš sistem »počepnik« pri polovičnih vrednostih. Kot kaže Slika 2, je temu približno tako, saj je prišlo do eksponentnega povečevanja latenc in s tem močnega upada prepustnosti pri približno 60 % obremenitvi, ko smo pošiljali s hitrostjo 7 TPS. Z modro vidimo prepustnost pri meritvi omrežja z velikostjo bloka 100 Tx, z zeleno pa prepustnosti pri 2-kratni velikosti bloka: 200 Tx.



Slika 2. Prepustnost v odvisnosti od obremenitve pri 2-kratni velikosti bloka.

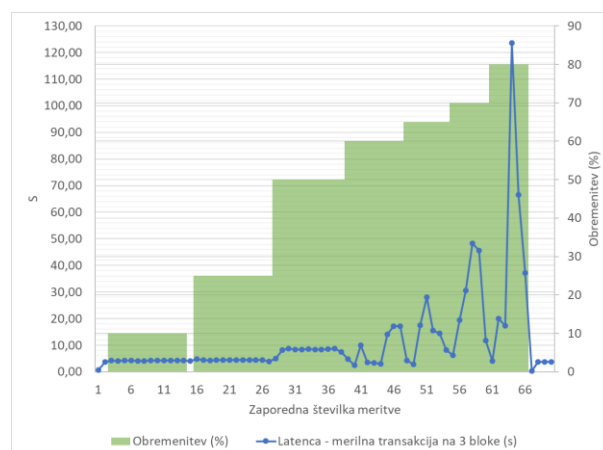
Na račun veriženja blokov do take spremembe v povečanih zakasnitvah ne bi smelo priti, kot vidimo iz rezultatov meritev, pa je do tega prišlo. To potrjuje razlog, da smo prišli do omejitve s sistemskimi viri. Ključna ugotovitev in napotek je, da Ganache okolje ni najbolj primerno za delovanje ob velikih obremenitvah, zato je potrebno biti pri uporabi ali analizi pozoren na smiselnost rezultatov.

## 4.2 Sondiranje omrežja

Na grafu (Slika 3) vidimo rezultate meritev latence pri sondiranju na vsak 3. blok. Z zelenimi stolpci je prikazana obremenitev, modra črta pa povezuje posamezne meritve latence.

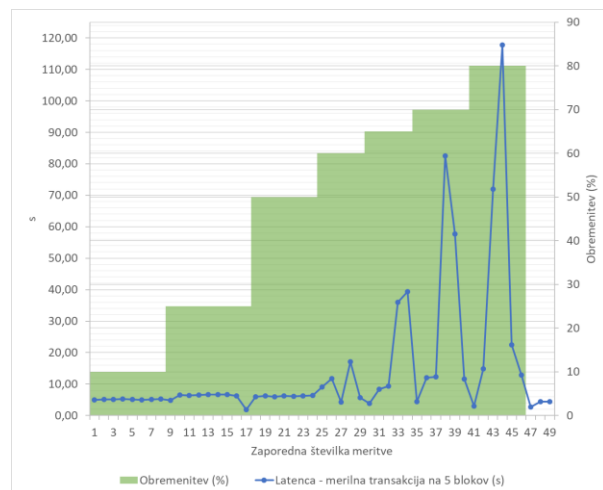
Opazimo, da na začetku, ko so obremenitve še relativno nizke, latenca počasi postopno narašča, kar je povsem pričakovano. Pri povečani obremenitvi, nekje nad 60 % pa se pojavi zanimiv pojav - vedno večja razpršenost in veliki naključni skoki meritev zakasnitev. To pomeni, da so nekatere transakcije praktično takoj

vključene v bloke, nekatere pa morajo zaradi velike obremenitve čakati dlje.



Slika 3. Sondiranje na vsak 3. blok.

Podobne rezultate in razpršenost pri povečani obremenitvi smo dobili tudi pri sondiranju na vsak 5. (Slika 4) oziroma na vsak 10. blok.



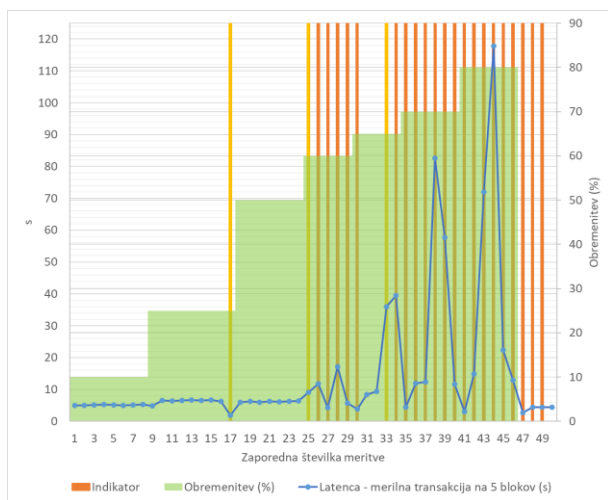
Slika 4. Sondiranje na vsak 5. blok.

Ti rezultati so nam dali idejo, da lahko sestavimo indikator, ki nas bo opozoril, ko bo prihajalo do preobremenitve. S pomočjo razmisleka in preizkušanja na pridobljenem setu meritev smo sestavili indikator, ki ob vsaki novi meritvi uspešno zazna ali v omrežju prihaja do preobremenitev.

Psevdo koda indikatorja:

1. Izračunamo povprečje zadnjih 5 meritev sondiranja, vključno s trenutno meritvijo
2. Izračunamo varianco med trenutno meritvijo in povprečjem zadnjih 5 meritev
3. Izračunamo standardni odklon
4. Izračunamo kolikšen odstotek od trenutne meritve, predstavlja standardni odklon
5. Dodamo logiko za opozorilo: če dve zaporedni meritvi odstopata za več kot 15 % potem, je to alarm za prehod v zasičenje. Če za toliko odstopa le ena je to opozorilo za previdnost.

Delovanje indikatorja vidimo na grafu (Slika 5), kjer so poleg obremenitve (zeleni stolpiči) in latence (modra linija), dodani še rezultati, ki nam jih sporoča indikator: Oranžen stolpec pomeni opozorilo, rdeči stolpec pa alarm za prehod v preobremenitev.



Slika 5. Delovanje indikatorja pri sondiranju na vsak 5. blok.

Na ta način smo dobili učinkovit indikator, ki s posameznimi sondami in s tem minimalnim vplivom na omrežje, in relativno majhno zakasnitvijo (največ dve meritvi), uspešno definira mejo, ko v omrežju prihaja do preobremenitve.

## 5 Zaključek

Med preučevanjem zmogljivosti omrežja veriženja blokov s pomočjo orodja Hyperledger Caliper smo opazili določene izzive, s katerimi se srečujemo, na kakšne omejitve lahko naletimo in kako nam lahko orodje pomaga pri analiziranju in razvoju. Potrebno je biti pozoren, da pridobljene meritve kritično ocenimo in utemeljimo kaj in zakaj se dogaja v omrežju, ki ga analiziramo.

Skozi raziskavo smo uspešno preizkusili Hyperledger Caliper na emuliranem omrežju, spoznali omejitve našega modela, ko prihaja do povečanih obremenitev. Ključna ugotovitev, ki smo jo uspešno dokazali, je, da lahko že s posameznimi sondami in s tem minimalnim vplivom na omrežje ter hkrati tudi z minimalnimi stroški transakcij relativno uspešno zaznamo povečane obremenitve in prehajanje v zasičenje. To je za razliko od obremenitvenega testa veliko bolj primerna metoda diagnosticiranja omrežij blokovnih verig, saj jo lahko uporabimo v »živih«, javnih omrežjih in ne le na modelu, ki smo ga uporabili v sklopu naše raziskave. S tako metodo lahko že z eno sondo, ki jo pošljemo v omrežje vsakih nekaj blokov, iz analize prejšnjih meritev, razberemo, kdaj je omrežje preobremenjeno in posledično prihaja do velike razpršenosti zakasnitev. Naš indikator tako predstavlja

praktično rešitev za zaznavanje povečane obremenitve v omrežjih blokovnih verig.

Nadaljnji koraki pri naši raziskavi, bi lahko vključevali preizkus lokalnega ali testnega Ethereum omrežja in nadaljnji razvoj našega indikatorja za zaznavanje obremenitev do te mere, da bi v realnem času diagnosticirali javna omrežja. Z orodjem Caliper bi se lahko osredotočili tudi na porabo virov, simulacijo realnih aplikacij in s tem nadgradili naš obremenitveni test.

Izziv zmogljivosti v kontekstu tehnologij porazdeljenih evidenc še zdaleč ni rešen, se pa pojavlja vedno več različnih pristopov in rešitev k skaliranju zmogljivosti (angl. Performance scaling). Te rešitve lahko v splošnem razdelimo v dve skupini: tiste, ki razširjajo osnovne verige (angl. Layer 1 scaling) in razširjanje z uvedbo ločenih verig/rešitev (angl. Layer 2 scaling). V prvo skupino spadajo rešitve, ki vključujejo različno velikost in frekvenco blokov, različne konsenzne mehanizme, alternativne podatkovne strukture in razdelitev na dele (angl. Sharding). V nadaljevanju bi se lahko dotaknili tudi analize in rešitev v drugem sloju, kamor spadajo: stranske verige (angl. Sidechains), kanali stanja (angl. State channels), plazemske verige in različne vrste zavrtkov (angl. Rollups). Tema zmogljivost je v sklopu tehnologij razpršenih evidenc zelo aktualna, področje je še relativno mlado in zato je razumevanje tematike, poznavanje orodji, kot je Hyperledger Caliper koristno in priročno za razvijalce ter raziskovalce na tem področju.

## Literatura

- [1] M. Pustišek, N. Živić in A. Kos, Blockchain : Technology and Applications for Industry 4.0, Smart Energy, and Smart Cities. Deutsche Nationalbibliothek, 2021.
- [2] C. Fan, S. Ghaemi, H. Khazaei in P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," IEEE, vol. 8, str. 126927–126950, 2020
- [3] J. Bonneau, "Why blockchain performance is hard to measure." Dosegljivo: <https://rb.gy/1nlu7>. [Dostopano: 23. 5. 2023]
- [4] M. Schäffer, M. di Angelo in G. Salzer, "Performance and Scalability of Private Ethereum Blockchains," Springer International Publishing, vol. 361, str. 103–118, 2019
- [5] Hyperledger, "Hyperledger caliper documentation." Dosegljivo: <https://hyperledger.github.io/caliper/v0.5.0/getting-started/>. [Dostopano: 24. 5. 2023]