https://doi.org/10.37528/FTTE/9788673954165/POSTEL.2022.023

SAOBRAĆAJNI MODELI *BLOCKCHAIN* SISTEMA

Zoran Bojković, Bojan Bakmaz
[1]Univerzitet u Beogradu, z.bojkovic@yahoo.com
[2] Univerzitet u Beogradu - Saobraćajni fakultet, b.bakmaz@sf.bg.ac.rs

Rezime: *Blockchain tehnologija otvorila je nove mogućnosti u digitalnom okruženju, uključujući distribuiranu verifikaciju podataka bez ovlašćenog entiteta, što je od velikog značaja za razmenu resursa. Veliki broj radova iz dostupne naučne literature posvećen je mogućnostima primene i poboljšanja performansi mehanizama za postizanje konsenzusa, dok istraživanja relativno ograničenog obima tretiraju saobraćajne modele od značaja za analizu i optimizaciju blockchain sistema. U radu su analizirani saobraćajni modeli kompleksnije teorijske osnove, koji mogu poslužiti kao solidan osnov za dalja istraživanja, sa posebnim akcentom na bitne parametre kojima se određuju performanse blockchain sistema.*

Ključne reči: *blockchain*, saobraćajni modeli, sistemi opsluge.

1. Uvod

Blockchain tehnologija, inicijalno osmišljena kao potpuno distribuirana baza podataka finansijskih transakcija u domenu kripto ekonomije, danas podrazumeva sisteme za digitalno upravljanje različitim vidovima resursa (nekretnine, intelektualna svojina, električna energija, radio spektar i sl.). Ovi sistemi su već iskazali veliki potencijal u sferama kao što su logistika [1], transport [2], zdravstvo [3] itd. *Blockchain* tehnologija koristi infrastrukturu i resurse savremenih informaciono-komunikacionih sistema, a u isto vreme može imati značajnu ulogu u optimizaciji funkcionisanja i povećanju bezbednosti istih, formirajući tako relaciju međusobne dobrobiti (tj. simbioze) [4-6]. Od velikog značaja je i uloga ove tehnologije u virtualizaciji i alokaciji resursa u savremenim komunikacionim mrežama [7].

Značajan broj radova iz dostupne literature posvećen je mogućnostima primene *blokchain* tehnologije, unapređenju mehanizama za postizanje konsenzusa, kao i bezbednosti informacija, dok je za sada skromniji opseg istraživanja usmeren ka teorijskom aspektu razvoja saobraćajnih modela. Saobraćajni modeli imaju primarnu ulogu u određivanju performansi sistema. Kao najznačajniji parametri izdvajaju se srednji broj transakcija na čekanju, srednje vreme potvrde transakcija, srednji broj transakcija po bloku.

Posle uvoda, u prvom delu rada predstavljeni su osnovni principi funkcionisanja *blokchain* sistema, dok je ostatak rada posvećen najinteresantnijim predloženim modelima opsluge koji se mogu primeniti u ovoj problematici. To su klasični modeli

opsluge sa čekanjem, jednofazni i dvofazni, sa eksplicitnim rešenjima ili sa potrebom simulacionog rešavanja, pri čemu je poseban izazov priprema polaznih saobraćajnih parametara modela, tako da ceo proces simulacije što realnije odražava saobraćajnu osobenost *blockchain* tehnologije. Rad je poučno-preglednog karaktera, dovodi do odgovarajućih zaključaka i usmerava ka daljim istraživanja.

2. Principi funkcionisanja *blockchain* sistema

Blockchain mrežu čine čvorovi koji generišu (iniciraju) i verifikuju transakcije (zahteve). Transakcije predstavljaju apstrakciju interakcije među korisnicima i kontinualno se generišu. Podaci o verifikovanim transakcijama čuvaju se u blokovima distribuiranim po čvorovima, formirajući linearnu sekvencu (lanac). Čvorovi mogu čuvati kompletnu repliku lanca blokova. Svaki blok predstavlja paket podataka sa zaglavljem i sadržajem. Zaglavlje sadrži meta podatke koji se odnose na identifikaciju bloka, kriptovanu vrednost bloka i prethodnog bloka (Merkleovo stablo), vremenski žig (*timestamp*), jednokratni slučajan broj (*nonce*), itd. Sadržaj bloka čine podaci o transakcijama. Pri generisanju bloka određeni čvorovi selektuju grupu transakcija koje su smeštene u privremenoj memoriji (*memory pool*). Veličina bloka direktno određuje broj transakcija koje mogu da se validiraju. Posle validacije, u procesu "rudarenja" (*mining*), blok se pridružuje lancu. *Blockchain* sistemi se direktno oslanjaju na kriptografske tehnike, kako bi se osigurao integritet podataka, naročito u okruženjima gde "poverenje" među čvorovima nije unapred uspostavljeno.

U zavisnosti od otvorenosti pristupa razlikuju se javne i privatne platforme. Tip platforme u značajnoj meri utiče na saobraćajne performanse sistema. Kod javnih *blockchain* platformi (npr. *Bitcoin*) bilo koji čvor u mreži je ovlašćen da generiše i verifikuje transakcije, kao i da dodaje blokove u lanac. Ovakva otvorenost sistema svakako je privlačna za potencijalne napadače, ali se to kompenzuje robusnim kriptografskim mehanizmima za verifikaciju, što sa druge strane negativno utiče na energetsku efikasnost i saobraćajne performanse zbog značajnog povećanja vremena opsluge. Kod široko primenjene SHA-256 heš (*hash*) funkcije vreme kriptovanja bloka je reda minuta, dok kriptovanje sa *ethash* funkcijom, primenjeno kod *Ethereum* platforme, traje nekoliko sekundi. Kod privatnih platformi (npr. *Hyperledger Fabric*) pristup sistemu je kontrolisan, dok samo određeni broj čvorova ima privilegije za validaciju transakcija. Ograničeni broj čvorova doprinosi povećanju skalabilnosti sistema, pri čemu i saobraćajne performanse mogu biti značajno unapređene. Takođe, moguće je identifikovati i konzorcijumski tip *blockchain* platformi, kao oblik delimično privatnog okruženja, sa jedinstvenim entitetom koji je odgovoran za postizanje konsenzusa i validaciju [8].

3. Osnovni modeli sistema sa čekanjem

Uobičajeno je i praktično da se modeli opsluge (*serving, queueing models*) tretiraju kao sistemi sa čekanjem ili sistemi bez reda čekanja, pri čemu i jedni i drugi mogu biti sa gubicima zahteva ili bez gubitaka zahteva. Najpoznatiji saobraćajni model bez čekanja je Erlangov (M/M/s/s(0)) model, odnosno Erlangova B formula gubitaka, sa osnovnim parametrima: ponuđeni saobraćaj, broj kanala (servera) u sistemu i gubici zahteva (GoS – *Grade of Service*). Na osnovu ovih, moguće je definisati i matematički

izraziti i druge parametre sistema. Pokazano je da rešenja modela, osim za eksponencijalnu raspodelu vremena opsluge (M), važe i za proizvoljnu raspodelu sa konačnom srednjom vrednošću (GI – *General Independent, renewal*). Pri beskonačnom broju kanala ovaj model se ponaša kao Poasonov.

Od modela sa čekanjem takođe prednjači Erlangov drugi model (M/M/s, M/M/s/∞, za $s > y$, što je uslov stabilnosti) i Erlangova C formula, koja izražava verovatnoću čekanja zahteva (gubitak po vremenu, verovatnoću blokiranja). U sistemu sa beskonačnim redom čekanja nema gubitaka zahteva, a osnovni parametri su kao u prvom modelu. Za proračune u samom redu čekanja često je potrebno poznavanje i intenziteta dolaznog toka zahteva ili pak intenziteta opsluge, što ne karakteriše sisteme bez čekanja.

Erlangov model sa čekanjem je izuzetno fleksibilan, jer se od njega mogu razviti na desetine modela, posebno na bazi selekcije korisnika iz reda za čekanje, u skladu sa odgovarajućom politikom, odnosno disciplinom pristupanja opsluzi. Odgovarajući model sa konačnim redom čekanja (M/M/s//L) je kompleksniji, ali takođe ima eksplicitno rešenje. L je broj mesta u redu ili se tretira zbirno sa kanalima, posebno kada je $s = 1$. Za konačni red čekanja, osim politike pristupa na opslugu, bitno je i pravilo napuštanja reda čekanja (*drop rule*).

Za sisteme sa čekanjem moguće je definisati veći broj parametara, poput srednjeg broja zahteva u redu i sistemu, srednjeg vremena čekanja ili boravka u sistemu, srednjeg vremena u redu za zahteve koji čekaju, raspodele vremena čekanja, verovatnoće čekanja većeg od nekog vremena i slično. Najprirodnije i najlakše za rešavanje je pravilo pristupanja opsluzi po redosledu dolaska u sistem (FCFS, *First Come First Served*), što u slučaju Erlangovog drugog modela rezultira eksplicitnim rešenjima, a već pri slučajnom izboru iz reda rešavanje modela po pitanju saobraćajnih parametara u samom redu se komplikuje.

Između Prve i Druge Erlangove formule (formule B i C) postoje skladne relacije

$$C(s,y) = \frac{sB(s,y)}{s - y(1 - B(s,y))} = \left[\frac{1}{B(s,y)} - \frac{1}{B(s-1,y)} \right]^{-1}, \qquad (1)$$

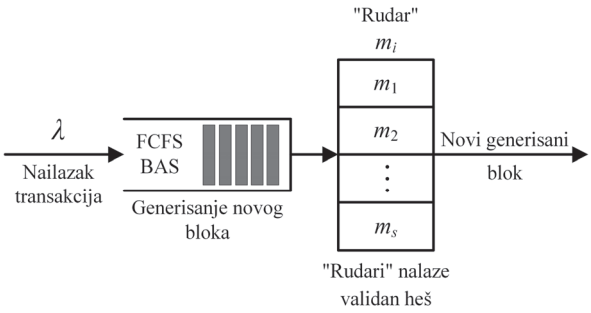
gde su: $B(s, y)$ i $C(s, y)$ – gubici po Prvoj, odnosno Drugoj Erlangovoj formuli, y – ponuđeni saobraćaj, a s – broj kanala u sistemu.

Vidi se da je gubitak po vremenu u Drugoj formuli veći od onog u Prvoj, a interesantno je da bi gubitak definisan po Poasonovoj raspodeli bio između prethodna dva gubitka, što je dugo korišćeno za tretman ponovljenih zahteva. Interesantan je i pokušaj da se naziv Erlangova A formula veže za Palmov osnovni model čekanja sa napuštanjem reda (nestrpljivi korisnici).

4. Mogućnosti korišćenja osnovnih modela opsluge za *blockchain* sisteme

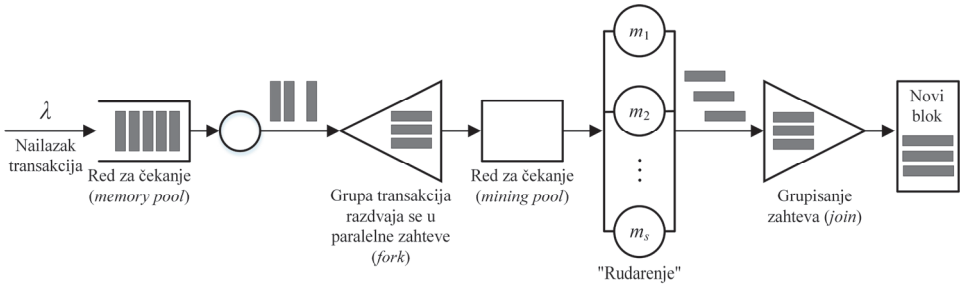
Blockchain sistemi su relativno neistraženi po pitanju teorijskog modelovanja, a postepeno se nameću modeli za simulaciju korišćenjem teorije sistema opsluge sa čekanjem. Osnovni modeli opsluge su jednofazni, sa jednodimenzionalnim grafom stanja za sisteme sa čekanjem (Markovljev *birth and death* proces), odnosno jednodimenzionalnim verovatnoćama stanja. Prirodno je da se za modelovanje *blockchain* sistema najpre koristio M/M/1 model opsluge.

U radu [9] vršena je simulacija *blockchain* platforme preko JMT (*Java Modelling Tools*) alata namenjenog za analizu performansi sistema opsluge sa redom za čekanje. Na Slici 1. prikazan je red čekanja i *s* "rudara", odnosno M/M/s/L model opsluge. Kapacitet (dužina) reda čekanja odgovara srednjem broju transakcija po bloku (Tx_B), politika prihvatanja iz reda radi opsluge je FCFS, a pravilo napuštanja reda je BAS (*Block After Service*). Ovde se određeni broj transakcija smešta u memoriju čvorova "rudara", dok ostale transakcije, iako obrađene, ostaju u redu za čekanje (*mempool*-u).



Slika 1. M/M/s/L sistem opsluge "rudarenjem"

Nešto kompleksniji sistem realizovan je kombinacijom M/M/1 i M/M/s modela [10]. Prvi model poslužio je kao memorijski *pool*, dok je *fork-join* set omogućio *batch* generisanje, a drugi model predstavlja proces "rudarenja" (Slika 2). Predloženi sistem je jednostavno, ali zadovoljavajuće sredstvo za procenu i prikaz mnogih važnih indikatora, kao što su: (*a*) broj transakcija po bloku, (*b*) vreme "rudarenja" svakog bloka, (*c*) propusnost sistema izražena preko broja transakcija u jedinici vremena, (*d*) broj redova za čekanje, (*e*) vreme čekanja u redu, (*f*) broj nepotvrđenih transakcija u celom sistemu, (*g)* ukupan broj transakcija i (*h*) broj generisanih blokova.



Slika 2. Blok dijagram simulacije kombinacije M/M/1 i M/M/s modela

Predloženi model takođe je simuliran primenom JMT alata i korišćen je za procenu idealne jednodnevne statistike transakcije u *Bitcoin* platformi. Zatim je model iskorišćen za simulaciju dvomesečne stvarne statistike *Bitcoin* i *Ethereum* platformi. Iako se model koristio za procenu parametara od značaja za kriptovalute, mišljenje je samih autora da je u stanju da simulira i druge *blockchain* sisteme koji se ne zasnivaju na monetarnim transakcijama.

5. Dvofazni modeli *blockchain* sistema

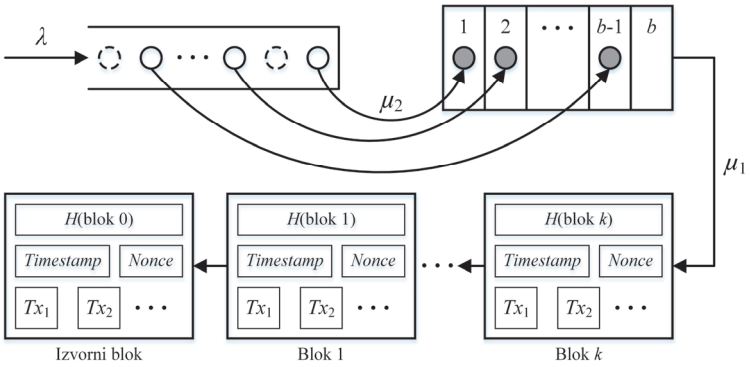
Za višefazne modele opsluge od posebnog interesa su raspodele faznog tipa, *PH*. Ove raspodele karakterišu se Markovljevim lancem sa kontinualnim vremenom, sa stanjima (fazama) 1,..., *k* i tranzicionom matricom verovatnoća *P*. Vreme boravka u stanju *i* eksponencijalne je raspodele sa srednjom vrednošću $1/\lambda_i$, a Markovljev lanac je ušao u stanje *i* sa verovatnoćom p_i. Slučajna promenljiva predstavlja ukupno vreme koje je proteklo od ulaska u Markovljev lanac do izlaska iz njega, a njena je raspodela faznog tipa. Osnovne raspodele se sreću pod nazivima: Erlangova-k, hipereksponencijalna, Koksova-k, hipererlangova i pogodne su za fitovanje.

Za potrebe simuliranja dvofaznih modela *blockchain* sistema u dostupnoj literaturi korišćeni su sistemi opsluge Markovljevog tipa GI/M/1 i M/PH/1 [11, 12].

5.1. GI/M/1 model

Prihvatljivo je da se *blockchain* može opisati kao Markovljev *bach* (grupni) sistem opsluge sa dve različite faze. Rad [13] razmatra GI/M/1 model, pri čemu je vreme potrebno za potvrdu transakcije posmatrano kroz dve faze opsluživanja, od kojih se jedna odnosi na generisanje samog bloka, a druga na uvođenje bloka u lanac. Vremena opsluge su eksponencijalno raspodeljena. Model je jednostavniji u slučaju eksponencijalne raspodele vremena između zahteva, odnosno Poasonovskog nailaska zahteva.

Kada se koristi sistem opsluge za modelovanje *blockchain* platformi, to predstavlja rešenje za postavku procesa opsluge analizom tehnike "rudarenja", koja se odnosi na konsenzus mehanizam. Ovde se za vreme opsluge uzima transakciono – konfirmaciono vreme, koje je suma vremena generisanja bloka i formiranja *blockchain*-a, odnosno vreme opsluge je dvofazno. Prva faza se generiše procesom "rudarenja", dok druga nastaje zbog mrežnog kašnjenja (*latency*).



Slika 3. Blockchain dvofazni model opsluge

Slika 3. ilustruje Markovljev *batch* proces sa dve različite faze opsluge. Transakcije stižu u *blockchain* sistem u skladu sa Poasonovim procesom i sa intenzitetom dolaznog toka (*arrival rate*) λ. Svaka transakcija mora najpre da uđe u red (čekaonicu, memoriju) beskonačnog (dovoljnog) kapaciteta. U procesu opsluge čeka da bude uspešno "rudarena" u blok, što se smatra prvom fazom opsluge, odnosno generisanje bloka. U

prvoj fazi nanovo generisani blok je potvrđen rešavanjem proračunski zahtevnog problema pomoću kriptografskog heš algoritma ("rudarenje"), a određeni čvorovi, koji se nadmeću za nalaženje odgovora, smatraju se "rudarima". Pobedniku će biti dodeljena nagrada koja se sastoji od nekih fiksnih vrednosti i naknada transakcija uključenih u blok, koji i dalje ima pravo da veže novi blok u lanac. Druga faza podrazumeva isključivo vreme potrebno za dodavanje bloka u lanac.

Kako bi se prevazišli bezbednosni izazovi, maksimalna veličina bloka (b) izražena u broju transakcija je unapred određena, što je odlika *batch* sistema opsluge. Uz ovu pretpostavku, za model GI/M/1 postoji uslov stabilnosti (pozitivne rekurentnosti)

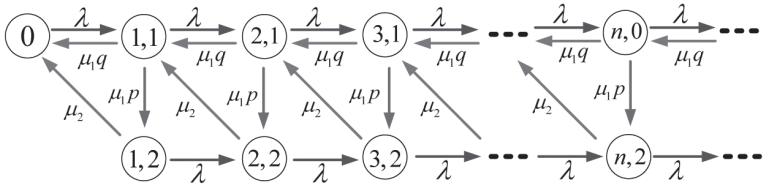
$$\frac{b\mu_1\mu_2}{\mu_1+\mu_2} > \lambda\,, \tag{2}$$

pri čemu je μ_2 intenzitet opsluge u prvoj fazi (i odgovara vremenu generisanja bloka), a μ_1 predstavlja intenzitet opsluge u drugoj fazi (i odgovara vremenu ulančavanja bloka). Podrazumevano je da su sve promenljive međusobno nezavisne. Primenom matrično-geometrijskog rešavanja sistema [14] preko vektora verovatnoća stanja, mogu se odrediti srednji broj transakcija u redu, srednji broj transakcija u bloku i srednje vreme potrebno za potvrdu transakcija.

5.2. Modeliranje PBFT konsenzus mehanizma

Proteklih nekoliko godina unapređenje mehanizama za postizanje konsenzusa sa aspekta bezbednosti predstavlja jedan od najvećih istraživačkih izazova. Kombinacija DPoS (*Delegated Proof of Stake*) i PBFT (*Practical Byzantine Fault Tolerant*) pristupa nametnula se kao ključni mehanizam za osiguravanje visoke bezbednosti *blockchain* sistema.

U skorašnjem radu [15] korišćen je M/PH/1 model opsluge radi analize performansi unapređenog PBFT mehanizma preko uslova stacionarnog stanja. Konsenzus se najčešće realizuje kroz tri faze. U prvoj fazi, primenom DPoS mehanizma, na osnovu performansi (npr. brzina generisanja bloka) i ostvarenog poverenja, delegiraju se čvorovi kandidati za ulogu "garanta" uspešnog generisanja bloka. U drugoj fazi, iz skupa delegiranih čvorova, određuje se grupa zadužena za generisanje bloka (primarna grupa) i grupa za verifikaciju blokova i identifikaciju malicioznih čvorova (alternativna grupa). Poslednja faza podrazumeva verifikaciju blokova PBFT konsenzusom u čvorovima alternativne grupe, pri čemu se degradiraju maliciozni čvorovi iz primarne grupe. Graf stanja i prelaza modela M/PH/1 prikazan je na slici 4. Ovaj model, sa odgovarajućim parametrima, usaglašen je sa predloženim unapređenim PBFT konsenzus protokolom.



Slika. 4. Graf stanja i prelaza za M/PH/1 model opsluge

Vreme postizanja konsenzusa okarakterisano je eksponencijalnim raspodelama sa dva različita parametra, a prostorno stanje pripada dvodimenzionalnom Markovljevom procesu. Stoga se ovo vreme može predstaviti preko dvodimenzionalne PH raspodele.

Ovde se dokazuje da je sistem stabilan (pozitivno rekurentan) ako za saobraćajno opterećenje ρ važi

$$\rho = \frac{(\mu_1 p + \mu_2)\lambda}{\mu_1 \mu_2} < 1, \tag{3}$$

pri čemu je λ ($\lambda > 0$) intenzitet dolazaka blokova koji sledi Poasonov proces, μ_1 ($\mu_1 > 0$) je parametar eksponencijalne raspodele, koji odgovara vremenu delegiranja čvorova, p je verovatnoća prelaska verifikovanog bloka iz sistema u *blockchain*, μ_2 ($\mu_2 > 0$) parametar eksponencijalne raspodele sekundarnog (ponovljenog) delegiranja. Od značaja je i verovatnoća prelaska bloka u proceduru ponovljenog delegiranja ($q = 1 - p$).

6. Zaključna razmatranja

U radu je izvršen kraći pregled bitnijih i dostupnih radova usmerenih na razvoj teorije redova čekanja *blockchain* sistema. Radi se o relativno skorijim istraživanjima, koja su sledila posle prikupljanja solidnih i kvalitetnih statističkih podataka o saobraćajnim parametrima praćenim tokom korišćenja ove tehnologije. Svrha rada je upoznavanje sa specifičnostima ove tehnologije, prednostima i problemima koje ona donosi. Za saobraćajni aspekt na raspolaganju stoje osnovni modeli sa čekanjem, eksplicitno rešeni i oni koji zahtevaju odgovarajuće alate za simulaciono modeliranje. Višefazni, konkretno dvofazni modeli su od trenutnog interesa i najnoviji kvalitetniji radovi su na tu temu. Ideja je i namera da se dostigne napredniji teorijski nivo sagledavanja i načina rešavanja aktuelnih problema i afirmišu sopstvene pretpostavke koje bi dovele do daljeg približavanja matematičke interpretacije realnom stanju odvijanja *blockchain* saobraćaja.

Literatura

[1] P. Dutta, et al., "Blockchain technology in supply chain operations: Applications, challenges and research opportunities", *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, Oct. 2020. DOI: 10.1016/j.tre.2020.102067

[2] D. Cocîrlea, et al., "Blockchain in Intelligent Transportation Systems", Electronics, vol. 9, no. 10, Oct. 2020. DOI: 10.3390/electronics9101682

[3] A. Tandon, et al., "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda", *Computers in Industry*, vol. 122, Nov. 2020. DOI: 10.1016/j.compind.2020.103290

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things", *IEEE Access*, vol. 4, 2016, pp. 2292-2303. DOI: 10.1109/ACCESS. 2016.2566339

[5] C. V. N. U. B. Murthy, et al., "Blockchain based cloud computing: Architecture and research challenges", *IEEE Access*, vol. 8, pp. 205190-205205, 2020. DOI: 10.1109/ ACCESS.2020.3036812

[6] G. Praveen, et al., "Blockchain for 5G: A prelude to future telecommunication", *IEEE Network*, vol. 34, no. 6, pp. 106-113, Nov./Dec. 2020. DOI: 10.1109/MNET.001.2000005

[7] Z. Bojkovic, B. Bakmaz, "Blockchain-enabled network slicing", *Proc. 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, Oct. 2021, pp. 203-208, DOI: 10.1109/TELSIKS52058.2021.9606300

[8] D. Puthal, et al., "Everything you wanted to know about the Blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6-14, July 2018. DOI: 10.1109/MCE.2018.2816299

[9] R. A. Memon, et al., "Modeling of blockchain based systems using queuing theory simulation", *Proc. 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 107-111, 2018. DOI: 10.1109/ICCWAMTIP.2018.8632560

[10] R. A. Memon, P. L. Jian Ping Li, J. Ahmed, "Simulation model for blockchain systems using queuing theory", *Electronics*, vol. 8, no. 2, 234, 2019. DOI: 10.3390/electronics8020234

[11] H. Akimaru, K. Kawashima, *Teletraffic: Theory and Application*, London, UK: Springer, 1993.

[12] V. B. Iversen, *Teletraffic Engineering and Network Planning*, Department of Photonics Engineering, Technical University of Denmark, 2015.

[13] Q-L. Li, J-Y. Ma, Y-X. Chang, "Blockchain queue theory", in X. Chen, et al., *Computational Data and Social Networks* (*CSoNet* 2018), *Lecture Notes in Computer Science*, vol. 11280, Cham, Germany: Springer, 2018, DOI: 10.1007/978-3-030-04648-4_3

[14] M. F. Neuts, *Matrix-Geometric Solutions in Stochastic Models: An Algorithmic Approach*, Johns Hopkins University Press,1981.

[15] F-Q. Ma, R-N. Fan, "Queuing theory of improved practical Byzantine fault tolerant consensus", *Mathematics*, vol. 10, no. 2,182, 2022. DOI: 10.3390/math10020182

Abstract: *Blockchain technology has opened the door to new opportunities in the digital environment, including distributed data verification without an authorized entity, which is of great importance for asset exchange in a real life. Numerous papers in the open literature are dedicated to the application possibilities and performance improvement of consensus mechanisms. On the other hand, relatively limited attention has been devoted to the traffic models significant for the analyses and optimization of blockchain systems. In this paper, several traffic models, which can serve as a steady foundation to further research, are analyzed from the theoretical point of view. Relevant parameters for blockchain systems performance evaluation are emphasized, too.*

Keywords: *blockchain, queueing theory, teletraffic models.*

TRAFFIC MODELS FOR BLOCKCHAIN SYSTEMS

Zoran Bojkovic, Bojan Bakmaz