Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.3
DOI: https://doi.org/10.24867/19BE12Kupresanin

JEDNO REŠENJE LANCA-BLOKOVA

ONE SOLUTION OF BLOCKCHAIN

Tamara Kuprešanin, Miroslav Popović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Lanac-blokova u poslednje vreme privlači sve veću pažnju širom sveta zbog svog potencijala da obezbedi sigurnost i verifikaciju za različite vrste podataka pomoću decentralizovane mreže koja se ne može izmeniti. Iako je ova tehnologija prvobitno služila za kriptovalute, vremenom je našla primenu u različitim oblastima, od zdravstva, transporta do umetnosti. U ovom radu je predstaljena implementacija lanca-blokova, u Python-u, koja omogućava stvaranje i verifikaciju transakcija, njihovo dodavanje u blokove, koji se zatim međusobno digitalno povezuju. Eksperimentalni rezultati, koji su predstavljeni, pokazuju način na koji porast broja čvorova u mreži utiče na porast broja dodatih transakcija po sekundi u lanac-blokova.*

Ključne reči: *lanac-blokova, heš funcija, rudarenje, digitalno potpisivanje, internet stvari*

Abstract – *Blockchain has recently drawn more and more attention around the world because of its potential to provide security and verification for different types of data using a decentralized network that cannot be changed. Although this technology was originally used for cryptocurrencies, eventually it has found application in various areas, from healthcare to transportation and art. This paper presents our implementation of blockchain, in Python, which enables the creation and verification of transactions, their addition to blocks, which are then digitally interconnected. The experimental results, which are presented, show the way in which the increase in the number of network nodes affects the increase in the number of added transactions in the blockchain per second.*

Keywords: *blockchain, hash function, mining, digital signiture, internet of things*

1. UVOD

Lanac-blokova predstavlja bazu podataka ili javni zapisnik svih transakcija i digitalnih radnji koje su izvršene i deljene između učesnika. Svaka transakcija u ovoj bazi mora biti odobrena od većine učesnika u sistemu.

Jednom unešena informacija ne može nikada biti izbrisana, pa samim tim, lanac-blokova sadrži pouzdan i verifikovan zapis svake transakcije koja je ikada nastala. Svaka transakcija, ugovor, proces i izvršeni zadatak se digitalno potpisuju radi verifikacije i provere ispravnosti. Jedna od ključnih karakteristika lanca-blokova jeste da se ova digitalna knjiga ne čuva na jednom mestu, već na svim računarima koji čine potpuno povezanu mrežu.

Stuart Haber i W. Scott Stornetta su još 1991. osmislili koncept koji je kasnije poslužio kao inspiracija za stvaranje tehnologije lanca-blokova [1]. Pojedinac ili grupa pod nazivom Satoshi Nakamoto je 2008. u knjizi razvio osnovne koncepte tehnologije lanca-blokova i predstavio prvu upotrebu ove tehnologije stvorivši prvu kriptovalutu Bitcoin [2]. Ta inovativna tehnologija bazirala se na ključnim karakteristikama kao što su decentralizacija, postojanost, anonimnost i sigurnost. Iako je Bitcoin najpoznatija aplikacija lanca-blokova, ova tehnologija može se primeniti u različitim aplikacijama izvan kriptovaluta, kao što su pametni ugovori, javne usluge, internet stvari i službe bezbednosti. Tako na primer, S. Simić, M. Marković, S. Gostojić su u svom radu predstavili primenu pametnih ugovora u hotelijerstvu [3]. Dok Wang, Su, Zhang daju zanimljivu mogućnost primene ove tehnologije u internetu stvari za transport energije pomoću električnih vozila [4]. Al-Jaroodi, Mohamed predstavili su prednosti i izazove korišćenja lanca-blokova za finansijske, zdravstvene, energetske, telekomunikacione i zabavne aplikacije [5]. Sličnu studiju su sproveli i prikazali u svom radu Jaoude, Saade [6]. Dok je Hölbl sproveo sistematski pregled lanca-blokova u zdravstvu [7]. Danas tehnologija lanca-blokova ostaje otvorena za nova istraživanja i razvoj u industriji i akademskoj zajednici.

Ovaj rad predstavlja proširenu verziju početnog rada Daniela van Flymen-a [8]. U svom radu Daniel je omogućio stvaranje jednostavnog lanca-blokova, dodavanje inicijalnog praznog bloka, stvaranje novih transakcija i njihovo dodavanje u blokove, izračunavanje heš funkcija blokova i dodavanje blokova u lanac, kao rešenje konsenzusa pronalazi se najduži lanca od ponuđenih. Za komunikaciju sa lancem koristio je HTTP zahteve, GET i POST. Kasnije je svoju ideju proširio i izmenio u knjizi [9].

U ovom radu uveden je serverski proces rukovalac koji omogućava prijavljivanje unapred određenog broja čvorova, čuvanje svih adresa i njihovo prosleđivanje prijavljenim čvorovima. Komunikacija čvorova se odvija na nivou transportnog sloja pomoću TCP protokola. Čvorovi se povezuju u potpuno povezanu mrežu. Svaki čvor osim, gore navedenih, osnovnih funkcionalnosti ima dodate mogućnosti: generisanje privatnog i javnog ključa, digitalnog potpisivanja transakcija pomoću privatnog ključa, verifikaciju pristiglih transakcija na osnovu javnog ključa pošiljaoca pre njihovog hronološkog dodavanja u blok, rudarenje slučajnog broja (engl. nonce – number once) i validaciju slučajnog broja. Za generisanje ključeva

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Miroslav Popović, red. prof.

implementiran je RSA algoritam, koji koristi Miler-Rabinov test za potrebe pronalaženja velikih prostih brojeva [10,11]. Decentralizacija i sigurnost podataka obezbeđene su pomoću kriptografske heš funkcije, digitalnih potpisa i mehanizma konsenzusa. Ovi mehanizmi uz druge sigurnosne mehanizme (šifrovanje, pouzdano izvršno okruženje, itd.) mogu biti deo sigurnosnog sistema za različite aplikacije interneta stvari [12].

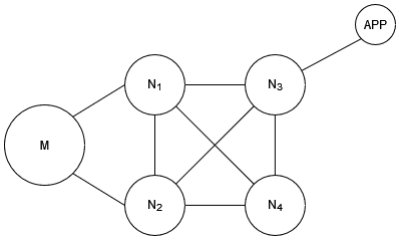
Ostatak rada organizovan je na sledeći način. U drugom odeljku predstavljena je arhitektura, ponašanje i implementacija sistema lanca-blokova. Opis testiranja i dobijeni rezultati dati su u trećem odeljku. Dok četvrti odeljak sadrži zaključak gde su opisane glavne prednosti i nedostaci konkretne implementacije i pravce daljeg razvoja.

2. ARHITEKTURA I IMPLEMENTACIJA

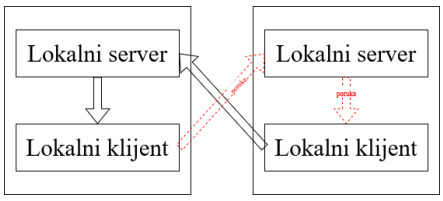
U ovom odeljku je prikazna je arhitektura, ponašanje i implementacija lanca-blokova.

2.1. Arhitektura

Arhitektura sistema na bazi lanca-blokova sastoji se od: jednog serverskog procesa rukovaoca (M), više čvorova (N_1 , N_2 ,...., Nn) i jedne ili više korisničkih aplikacija (APP), kao na slici 1. Rukovaoc je izveden iz klase BaseManager i služi za čuvanje adresa svih čvorova iz mreže. Čvorovi su realizovani pomoću procesa lokalnog klijenta i procesa lokalnog servera, videti sliku 2.

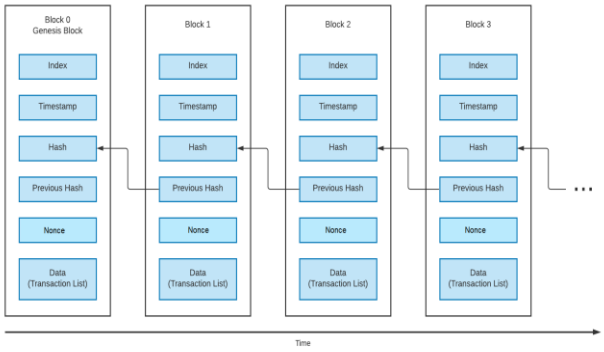


Slika 1. *Arhitektura sistema na bazi lanca-blokova*



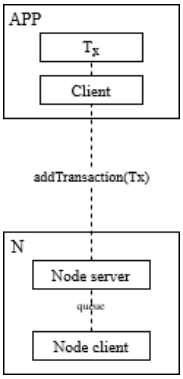
Slika 2. *Realizacija komunikacije čvorova*

Svaki čvor u mreži ima mogućnost stvaranja lanac-blokova koji se sastoji iz digitalno povezanih blokova. Primer lanca-blokova prikazan je na slici 3.



Slika 3. *Prikaz lanca-blokova*

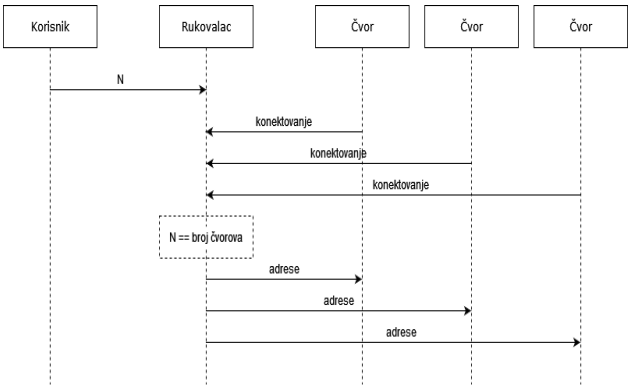
Čvorovi imaju mogućnost da stvaraju nove transakcije (T_x) pomoću funkcije addTransaction. Pojednostavljeni UML diagram je prikazan na slici 4.



Slika 4. *UML diagram klasa sistema na bazi lanca-blokova*

2.2. Ponašanje

Prilikom pokretanja rukovaoca potrebno je da korisnik zada broj čvorova koji će činiti mrežu. Čvorovi se povezuju sa rukovaocem, zapisujući svoje adrese, dok se ne dostigne željeni broj čvorova. Zatim svi čvorovi dobijaju informacije o adresama svih preostalih čvorova, videti sliku 5, i međusobno se povezuju u potpuno povezanu mrežu.



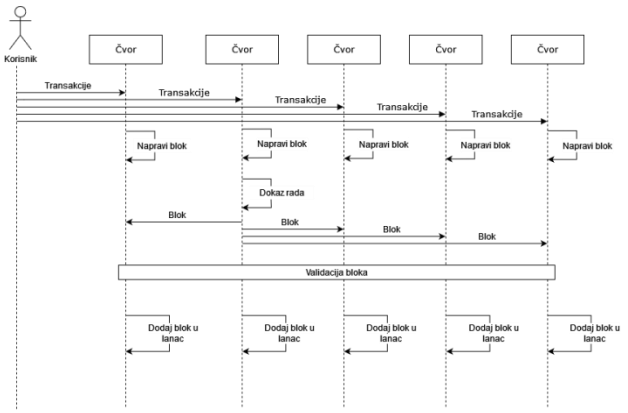
Slika 5. *Prijavljivanje čvorova rukovaocu*

Kada su čvorovi povezani i stvorena potpuno povezana mreža, svaki od čvorova stvara inicijalan prazan blok i čeka nove transakcije za stvaranje daljih blokova. Svaki blok se sastoji od: indeksa, transakcija, vremenske oznake kada je stvoren blok, slučajnog broja (engl. nonce), heš koda i heš koda prethodnog bloka. Ovi parametri su jedinstveni za sve blokove. Na slici 3 je prikazan lanac-blokova i način na koji se blokovi digitalno povezuju pomoću heš kodova.

Za stvaranje heš koda koristi se SHA-256 funkcija i podaci: indeks, transakcije, vremenska oznaka, slučajan broj (engl. nonce) i heš kod prethodnog bloka, što onemogućava promenu sadržaja jednog bloka, a da se ne promeni sadržaj svih blokova koji idu nakon njega. Korištena kriptografska heš funkcija je matematički algoritam koji mapira podatke proizvoljne dužine u izlaz dužine 256 bita.

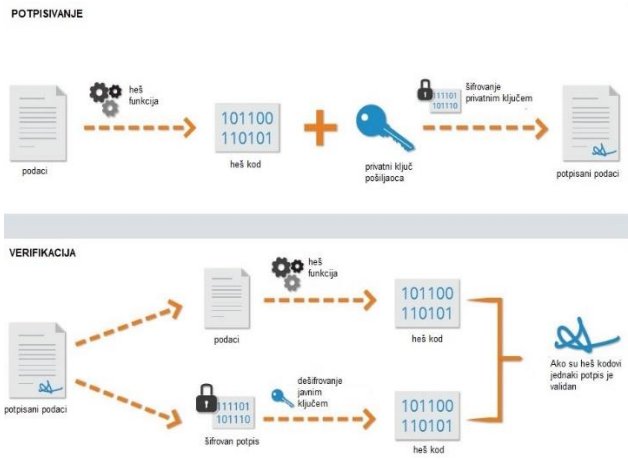
Slučajan broj (nonce) predstavlja broj koji rudari treba da pronađu da bi se dobio heš koji počinje sa unapred zadatim brojem nula. Kada je pronađen slučajan broj (engl. nonce) i napravljen novi blok, on se šalje ostalim

čvorovima u mreži na validaciju. Validacija bloka se vrši na osnovu slučajnog broja i heš funkcije. Kada je blok validiran on se dodaje na svim čvorovima u lanac. Proces dodavanja novih blokova i pronalaženja slučajne vrednosti predstavljen je na slici 6.



Slika 6. *Dodavanje blokova u lanac*

Svaka transakcija se sastoji od: pošiljaoca, primaoca, vrednosti i vremenske oznake (kada je nastala transakcija). Verifikovane transakcije se hronološki dodaju u novi blok. Verifikacija se vrši pomoću digitalnog potpisa sa privatnim i javnim ključem. Za generisanje ključeva implementiran je RSA algoritam. Prilikom pravljenja transakcija, čvor mora potpisati transakciju privatnim ključem, a prilikom prijema transakcije vrši se verifikacija na osnovu javnog ključa. Proces digitalnog potpisivanja i verifikacije prikazan je na slici 7.



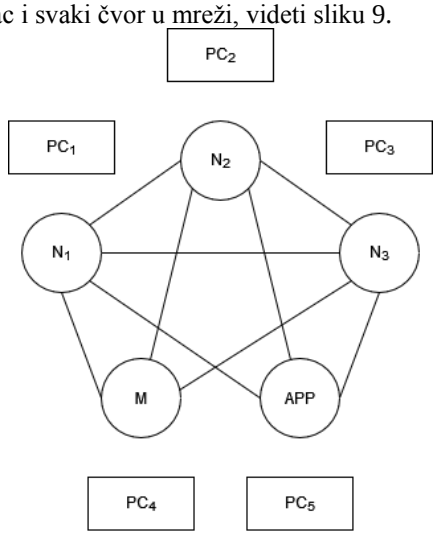
Slika 7. *Digitalno potpisivanje*

3. EKSPERIMENTALNA EVALUACIJA

Cilj ovog odeljka je da se pokažu dobijeni eksperimentalni rezultati, način na koji broj čvorova u mreži utiče na promenu broja dodatih transakcija u lanac-blokova.

Za potrebe testiranja napravljen je testni program *test*, koji služi za izračunavanje ostvarenog broja transakcija u sekundi. Eksperiment je vršen na potpuno povezanoj mreži sa 3, 5, 8, 10, 12 i 15 čvorova. Test program se povezuje sa rukovaocem, od kojeg saznaje informacije o broju čvorova i njihove adrese, zatim se sa čvorovima povezuje na isti način na koji se oni međusobno povezuju. Test aplikacija broj ponuđenih transakcija na ulazu, *num_trans* = [50, 150, 200, 350, 450, 550, 650, 700, 900], deli u odnosu na broj čvorova u trenutnoj mreži i prosleđuje dobijenu vrednost čvorovima. Čvorovi obavljaju uobičajene funkcije: stvaranja transakcija, digitalnog potpisivanja, prosleđivanja, verifikacije transakcija, dodavanja novih transakcija u blokove, verifikacije blokova i dodavanja blokova u lanac. Zatim nakon stvaranja lanca-blokova, čvorovi prosleđuju informacije o dužini lanca-blokova, kao i sam lanac-blokova.

Na osnovu informacija dobijenih sa svih čvorova aplikacija izračunava ostvarenu propusnost sistema. Deljenjem ukupnog broja transakcija i potrošenog vremena dobija se broj transakcija po sekundi. Eksperiment smo sprovodili na lokalnoj mreži u studentskoj laboratoriji. Test aplikacija se pokretala na zasebnom računaru, kao i rukovalac i svaki čvor u mreži, videti sliku 9.

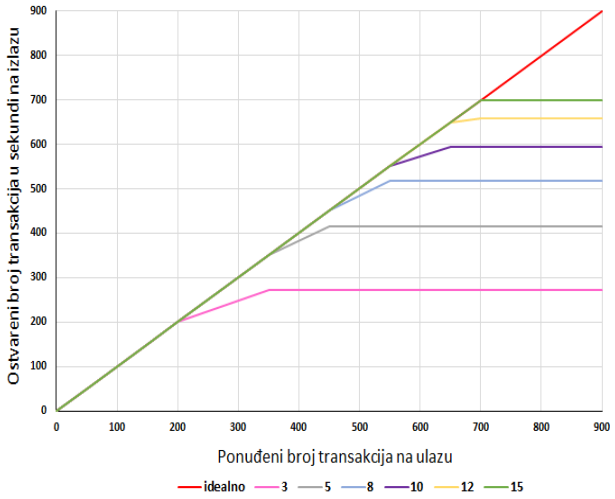


Slika 9. *Primer testne mrežne konfiguracije*

Karakteristike eksperimentale postavke su sledeće. Lan karakteristike: računarske utičnice su povezane na jedan prekidač Juniper EX-4300. Ovaj prekidač obezbeđuje korisničke pristupne portove od 10/100/1000Mbps i uplinkove od 10Gbps. Mrežni kablovi su UTP kategorije CAT5e. Karakteristike računara: CPU - Intel Corei7-10700 CPU @ 2.90GHz (8 cores x64), MB - Dell 0x8DxD, RAM - 2 module x 16 GB DDR4 @ 2666MHz, HDD - 1TB (Toshiba), Graphics - Intel(R) UHD Graphics 630. Verzija softvera: OS - Windows 10 Enterprise (x64). Python verzija 3.10.5 on win32.

Tabela 1. *Dobijeni eksperimentalni rezultati*

Čvorova / Transakcija	*3*	*5*	*8*	*10*	*12*	*15*
50	50	50	50	50	50	50
150	150	150	150	150	150	150
200	200	200	200	200	200	200
350	272	350	350	350	350	350
450	272	415	450	450	450	450
550	272	415	518	550	550	550
650	272	415	518	593	650	650
700	272	415	518	593	659	698
900	272	415	518	593	659	698



Slika 10. *Eksperimentalno dobijeni diagram*

Dobijeni eksperimentalni rezultati prikazani su u tabeli 1 i na slici 9. Sva testiranja su ponovljena 20 puta radi sigurnosti. U prikazanoj tabeli predstavljene su srednje vrednosti, odstupanja su bila zanemaljiva.

Kolone u tabeli 1 sadrže informacije o broju čvorova u mreži, dok nam redovi govore o ponuđenom broju transakcija. Tabela 1 nam daje pregled ostvarenog broja transakcija u sekundi na izlazu u zavisnosti od broja čvorova u mreži. Eksperimentalno je utvrđeno da povećanje broja čvorova u mreži rezultira povećanju broja dodatih transakcija u sekundi u lanac-blokova, što se vidi iz date tabele 1 i slike 10.

4. ZAKLJUČAK

U okviru ovog rada predstavljena je jedna implementacija lanca-blokova. Prikazana je arhitektura rešenja i način stvaranja potpuno povezane mreže pomoću serverskog procesa rukovaoca. Opisan je način stvaranja novih čvorova, njihovo povezivanje, stvaranje transakcija, njihovo dodavanje u blokove, dodavanje blokova u lanac i njihovo digitalno povezivanje. Prikazani su algoritmi koji se koriste za računanje heš vrednosti, generisanje privatnog i javnog ključa, digitalno potpisivanje transakcija, validaciju transakcija, pronalaženje slučajne vrednosti (engl. nonce), verifikaciju blokova, kao i konsenzus algoritam.

Glavno ograničenje prikazanog rešenja je što je unapred potrebno odreti broj čvorova koji će učestvovati u stvaranju mreže, taj broj korisnik prosleđuje rukovaocu prilikom njegovog pokretanja. Jednom kada je mreža stvorena i čvorovi povezani nije moguće dodavati nove čvorove u mrežu, iz čega proizilazi da nije postignuto potpuno dinamičko povezivanje čvorova.

Glavna prednost opisanog rešenje je što je lanac-blokova implementiran u Python-u bez upotrebe dodatnih paketa, predstavljajući potpuno nezavisno i samostalno rešenje. Nezavisnost od paketa i tehnika omogućava lako integrisanje ovog rešenja u druge programe i sisteme, predstavljajući osnovu za njegovo dalje dograđivanje.

Zbog korisnih osobina same tehnologije lanca-blokova i nezavisnosti ovog rešenja, moguća je njegova primena u različitim oblastima. Glavni pravac budućeg rada je upotreba lanca-blokova u internetu stvari i pametnim kućama. Jedna od ideja je da se rad primeni na električnim brojilima koji bi činili čvorove u mreži i upisivali svoje trenutne vrednosti.

5. LITERATURA

[1] Stuart Haber, W. Scott Stornetta, “How to Time-Stamp a Digital Document”, In *Journal of Cryptology*, Vol. 3, No. 2, pp. 99-111, 1991.
[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.
[3] S. Simić, M. Marković, S. Gostojić, “Smart Contract and Blockchain Based Contract Management System”, ECBS, 2021.
[4] Wang, Su, Zhang, “BSIS for Energy Delivery in Vehicular Energy Network”, *IEEE Transactions on Industrial Informatics*, Vol. 15, Iss. 6, June 2019.
[5] J. Al-Jaroodi, N. Mohamed, “Blockchain in Industries: A Survey”, *IEEE Access*, Vol. 7, 2019.
[6] J. A. Jaoude, R. Saade, “Blockchain Applications – Usage in Different Domains”, *IEEE Access*, Vol. 7, 2019.
[7] M. Hölbl, “A Systematic Review of the Use of Blockchain in Healthcare”, In *Journal Symmetry*, Vol. 10, Iss. 10, 2018.
[8]https://github.com/dvf/blockchain?ref=hackernoon.com (pristupljeno u martu 2021.)
[9] Daniel van Flymen, “Learn Blockchain by Building One: A Concise Path to Understanding Cryptocurrencies”, Apress, 2020.
[10] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, 1978.
[11] Rabin, Michael O., “Probabilistic algorithm for testing primality”, *Journal of Number Theory*, Vol. 12, No. 1, pp. 128–138, 1980.
[12] D. Minoli, B. Occhiogrosso, “Blockchain mechanisms for IoT security ”, In *Journal Internet of Things*, Vol. 1, pp. 1–13, 2018.

Kratka biografija:

Tamara Kuprešanin rođena je u Novom Sadu 1998. god. Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Računarska tehnika i računarske komunikacije odbranila je 2022. god.

kontakt: tamarakupresanin@gmail.com

Miroslav Popović rođen je u Novom Sadu 1961. Doktorirao je na Fakultetu tehničkih nauka 1990. god., a od 2002. je zvanju redovni profesor. Oblast interesovanja su sistemi zasnovani na računaru.