Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 626/627
DOI: https://doi.org/10.24867/26CG07Dzakula

ARHITEKTURA ETHEREUM 2.0

ARCHITECTURE ETHEREUM 2.0

Jelena Cupać, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO
Kratak sadržaj – *U radu su opisane faze ažuriranja Ethereum 1.0 mreže na Ethereum 2.0 mrežu. Radi demonstracije načina na koji se mogu inspektovati podaci na Ethereum mreži, kao što su izvršene transakcije i kreirani blokovi, korišćeni su istraživači blokova. Za kreiranje novčanika iskorišten je MetaMask, dok je kao istraživač blokova korišten EtherScan. Transakcije su izvršene i pregledane na testnoj mreži Sepolia.*
Ključne reči: *blokčejn, ethereum 1.0, ethereum 2.0, mehanizam dokaza o radu, Sepolia*
Abstract – *The paper describes the phases of updating the Ethereum 1.0 network to the Ethereum 2.0 network. To demonstrate how data on the Ethereum network can be inspected, such as performed transactions and created block, block explorers are used. MetaMask was used to create the wallet, while EtherScan was used as a block explorer. Transactions were executed and reviewed on the Sepolia test network.*
Keywords: *blockchain, ethereum 1.0, ethereum 2.0, proof of stake, Sepolia*

1. UVOD

Potreba za decentralizovanim novcem je više predstavljala teorijski koncept, sve dok u pretprošloj deceniji ovaj koncept postaje održiv, i to zahvaljujući Satoši Nakamotu i njegovom radu 2008. godine u kojem predstavlja *Bitcoin* i blokčejn tehnologiju. *Bitcoin* i blokčejn tehnologija su počeli da oblikuju i definišu nove aspekte u domenu računarstva i informacionih tehnologija.

Vremenom, počeli su da se razvijaju i drugi projekti zasnovani na blokčejnu, jedan od njih je i *Ethereum*. Danas, *Ethereum* je decentralizovana mreža čvorova koja održava zajednički pogled na globalno stanje i automatski izvršava programski kod kada su prethodno definisani uslovi ispunjeni – pametni ugovori. Kako je broj korisnika *Ethereum* mreža u stalnom porastu, postojala je potreba za stabilnijom i skalabilnijom mrežom. Upravo to je dovelo do ažuriranja mreže koje će se odigrati kroz tri faze.

Cilj rada jeste upoznavanje sa tri faze ažuriranja *Ethereum* 1.0 mreže na *Ethereum* 2.0 mrežu, kao i demonstracija načina inspekcije podataka na mreži korišćenjem istraživača blokova.

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

2. LANAC BLOKOVA - BLOKČEJN

Potreba da se dokumentima utvrdi autentičnost postoji odavno. Jedan od načina da se utvrdi da je dokument kreiran baš u onom trenutku u kojem autor tvrdi jeste oslanjanje na centralni autoritet u koji svi imaju poverenja. Drugi način ne zahteva centralni autoritet, već samo javno objavljivanje. Iako je moguće lažirati pečate, otvoriti dokument tako da se izbegne fizička zaštita, često je to nepraktično i zahteva vreme, što napadaču ne biva isplativo. Međutim, u digitalnom svetu kreiranje identičnih kopija i lažiranje dokumenata je gotovo trivijalno.

Problem autentičnosti je rešen kriptografijom i digitalnim potpisima. Kako bi se utvrdilo da je digitalni dokument objavljen u određenom trenutku, moguće je imati centralni autoritet i verovati njemu, kao što je slučaj kod digitalnih sertifikata ili je, pak, ovo moguće postići i bez centralnog autoriteta, i to najčešće ulančavanjem kriptografskih heš vrednosti dokumenata i javnim objavljivanjem ovako kreiranog lanca. Blokčejn spaja tehnologije digitalnih potpisa i metode za utvrđivanje hronologije izmena čime se formira poverljiv javni skup podataka.

2.1. Terminologija blokčejna

2.1.1. Distribuirani sistem

Distribuirani sistem je kolekcija autonomnih računarskih elemenata koji su krajnjem korisniku predstavljeni kao jedan koherentni sistem [1]. Elementi se nazivaju čvorovii deluju koordinisano kako bi ispunili zajedničke ciljeve.

2.1.2. Peer-to-peer sistem

Peer-to-peer (P2P) sistemi pripadaju decentralizovanom tipu sistema. Svi čvorovi u ovakvom sistemu su jednaki, zapravo, svaki čvor je istovremeno i klijent i server (engl. *servant*). Posao je raspoređen po čvorovima umesto da je za obavljanje posla zadužen svega jedan server što P2P sisteme čini otpornijim budući da nema jedinstvene tačke otkaza.

2.1.3. Blokčejn

Postoji nekoliko definicija blokčejna. Blokčejn je distribuirani deljeni registar transakcija. Blokčejn je jezgro *peer-to-peer* sistema koji je kriptografski bezbedan, nepromenljiv - u koji se podaci mogu samo dodavati, a ne mogu se brisati, niti menjati. Sa poslovnog stanovišta, blokčejn se može definisati kao platforma gde čvorovi mogu da razmenjuju dobra koristeći transakcije bez postojanja centralnog tela kojem strane veruju [2].

2.1.4. Adresa

Adresa je jedinstveni identifikator koji služi da se označi primalac i pošiljalac u transakciji. Najčešće su to javni ključevi.

2.1.5. Transakcija

Transakcija je osnovna jedinica blokčejna, transfer vrednosti sa jedne adrese na drugu. Transakcije se organizuju u blokove.

2.1.6. Blok

Više transakcija su organizovane zajedno u jedan blok. Blokovi se povezuju kako bi kreirali krajnji lanac blokova – blokčejn. Pored grupe transakcija, blok sadrži i vrednost koja se samo jednom upotrebljava (*nonce*), vremensku odrednicu, kao i heš vrednost prethodnog bloka (*hash pointer*).

2.1.7. Čvorovi

Čvorovi su jaki računari povezani na blokčejn mrežu u cilju obrade i verifikacije transakcija. Čvorovi u mreži mogu da obavljaju različite funkcije u zavisnosti od njihove uloge – predlažu/validiraju transakcije i sl.

2.2. Konsenzus mehanizmi

Konsenzus je proces dogovaranja oko konačnog stanja podataka između nepoverljivih čvorova. Postoji nekoliko konsenzus algoritama, od kojih su dva korištena u *Ethereum* mreži – mehanizam dokaza o radu (engl. *proof of work*) i mehanizam dokaza o udelu tj, posedovanju valute (engl. *proof of stake*).

2.2.1. Proof of work (PoW)

Mehanizam dokaza o radu je konsenzus algoritam koji se oslanja na dokaz da je dovoljno računarskih resursa utrošeno pre predlaganja bloka za dodavanje u blokčejn. Ovaj algoritam se naziva i rudarenje. Rudarenje je proces validiranja transakcija rešavajući jednačinu. *Nonce* je broj koji se vrti u rasponu od 0 do 232 u pokušaju da se nađe onaj za koji će heš bloka imati odgovarajuću vrednost (nižu od zadate). Upravo je ovo jednačina koju rudari treba da reše kako bi validirali blok. Heš funkcija koja se koristi je SHA256.

Kako su heš funkcije jednosmerne funkcije, rudari nemaju način da pretpostave kakvi su im ulazni podaci potrebni da bi dobili rezultat koji žele. Zato moraju da isprobavaju redom različite vrednosti *nonce* broja, jednu po jednu, da bi dobili željeni rezultat. Stoga je bitno imati jak hardver, jer se tako može više pokušaja napraviti za kraće vreme i time povećava šansu da baš on bude taj koji će prvi kreirati validan blok. Da bi se našli potrebni ulazni podaci koji daju odgovarajući rezultat neophodan je izuzetno veliki broj pokušaja, a da bi se taj veliki broj pokušaja odradio za kratko vreme, neophodna je velika procesorska snaga i velika količina rada. Zbog toga se ovaj algoritam za rudarenje naziva mehanizam dokaza o radu, jer je rudar morao da uloži veliku količinu rada da bi došao do rezultata.

Pre nego što se u blokčejn doda blok koji je rudar kreirao i koji zadovoljava potrebne uslove, on ga šalje ostatku mreže na proveru validnosti. Oni proveravaju da li se za ulazne podatke koje je on imao zaista dobija heš koji on tvrdi da je dobio i, ako se pokazalo da je bio u pravu, taj blok zvanično postaje sastavni deo blokčejna i rudar dobija svoju nagradu i proviziju od transakcija. Ako blok nije validan, mreža će odbiti taj blok.

2.2.2. Proof of stake (PoS)

Mehanizam dokaza o udelu, tj. posedovanju valute menja način na koji se verifikuje i dodaje novi blok, te se umesto potrebe za obavljanjem računarskog posla i rešavanja kriptografske jednačine primenjuje ulaganje, odnosno vlasnici ulažu svoj novac kako bi dobili priliku da kreiraju nove blokove i budu nagradjeni. Što više novca biva uloženo, veća je verovatnoća da će algoritam izabrati baš tog validatora za kreiranje novog bloka. Ukoliko je validator maliciozan, a doda transakciju u blokčejn koju drugi validatori smatraju neispravnom, može izgubiti deo sredstava koje je uložio. Blokove proverava više validatora, a kada određeni broj validatora potvrdi ispravnost bloka, blok se smatra finalnim.

3. ETHEREUM 1.0

Ethereum je decentralizovana blokčejn platforma koju pokreće kriptovaluta pod nazivom *Ether*, koja omogućava vršenje transakcija, korišćenje i čuvanje nezamenljivih tokena (NFT), igranje igrica, korišćenje društvenih mreža i još mnogo toga. Platforma podržava i decentralizovane aplikacije (DApps), decentralizovane finansije (DeFi), decentralizovane razmene (DEX).

3.1. Ethereum nalog

U *Ethereum* mreži postoje dva tipa naloga, oni koji su u eksternom vlasništvu (kontrolisani privatnim ključem) i ugovorni nalozi kontrolisani pametnim ugovorom. Nalozi u eksternom vlasništvu su npr. *Metamask* ili *Coinbase* novčanici. Ovi računi se identifikuju preko javnog ključa koji predstavlja njihovu adresu. Kod ugovornih naloga adresa se dobija od adrese kreatora naloga i *nonce* vrednosti. Svaki *Ethereum* nalog je sačinjen iz 4 dela [3]:

- *Nonce* – broj transakcija koje su poslate sa određenog naloga ili broj kreiranih ugovora određenog naloga. Garantuje da se svaka transakcija može precesuirati samo jednom.
- *Ether* balans – broj *Wei*-a koji se poseduje na nalogu.

Wei je najmanja jedinica *Ether* kriptovalute.

- Heš kod – heš vrednost EVM bajt koda naloga, to je kod koji se izvršava kada adresa računa dobija poruke. Koristi se Keccak-256 heš funkcija.
- *Storage root* – 256-bitna heš vrednost korena *Merkle Patricia* stabla koje predstavlja sadržaj naloga.

3.2. Transakcije

Transakcija je kriptografski potpisan set instrukcija. Ove instrukcije mogu da prenose *Ether* sa jednog računa na drugi ili da interaguju sa pametnim ugovorima na blokčejnu. Svaka transakcija se sastoji iz pet delova [3]:

- Primalac transakcije
- Količina *Ether*-a koja se šalje transakcijom
- *Nonce* – broj transakcije poslate od strane tog

pošiljaoca
- *Gaslimit* – maksimalan gas koji može da se potroši zaizvršenje transakcije
- *Gas price* - broj *wei*-a po jedinici gasa koje pošiljalacplaća
- Potpisani podaci kojima se identifikuje pošiljalac.

3.3. Konsenzus mehanizam

Ethereum 1.0 koristi PoW algoritam za validiranje transakcija. Čvorovi u mreži se takmiče ko će pre rešiti jednačinu i kreirati novi blok. Kao heš funkcija koristi se *Ethash* heš funkciju, dok se kao glavni resursi za rudarenje koriste grafičke procesorske jedinice - GPU.

4. ETHEREUM 2.0

Ethereum kao platforma omogućava korisnicima da kreiraju pametne ugovore. Pametni ugovori su sporazumi između dve strane koji treba da izvrše transakciju kada su uslovi koji su definisani na početku ispunjeni. Ovi ugovori se smatraju izuzetno bezbednima budući da se čuvaju na blokčejn mreži, nakon što su odobreni, repliciraju se po mreži što ih štiti od zlonamernih akcija i menjanja. To je doprinelo razvoju okruženja i to u pogledu korisnika, *Etherscan* procenjuje da postoji preko 231 miliona jedinstvenih adresa, aplikacija, i to se prognozira da će do kraja 2023. godine postojati oko 500 hiljada decentralizovanih aplikacija, i u pogledu ukupnog korišćenja, pri čemu broj transakcija dostigne 1.2 miliona na dnevnom nivou. Zbog svega navedenog, potreba za stabilnijom i skalabilnijom mrežom se samo povećavala. Stoga su programeri koji stoje iza *Ethereum*-a, zajedno sa Vitalikom Buterinom, konačno odredili datume za dugo očekivano ažuriranje glavne mreže.

Ažuriranje *Ethereum* 1.0 mreže je *Ethereum* 2.0, poznat i pod formalnim nazivom *Serenity* i bio je u planu od skoro samog nastanka *Ethereum*-a. Buterin je već na samom početku shvatio da će mali broj transakcija koje je Ethereum 1.0 sposoban da obradi u sekundi postati problem pre ili kasnije. Ovaj broj je iznosio svega 15 transakcija po sekundi, a to nije bilo dovoljno da se zadovolji vizija *Ethereum*-a kako bi podržao mnoštvo decentralizovanih aplikacija.

Ažuriranje na Ethereum 2.0 je predviđeno da se izvede u nekoliko faza, tačnije u tri, od kojih su dve već realizovane. Najvažnije promene predviđene 2.0 verzijom su orijentisane na poboljšanje skalabilnosti kako bi mreža mogla da podrži još veći broj korisnika i transakcija. Među promenama je i prelazak sa PoW mehnizma konsenzusa na PoS, u kojem će korisnici zalagati ETH kako bi postali validatori, umesto da se učešće u kreiranju blokova zasniva na procesorskoj moći sistema koji korisnik koristi. Još jedna promena bi bila i tranzicija sa jednog lanca blokova na 64 lanca koji se paralelno izvršavaju.

4.1. Faza 0

Faza 0 podrazumeva lansiranje *Beacon* lanca i prelazak sa PoW mehanizma konsenzusa na PoS, započeta je 1.12.2020. godine. U ovoj fazi potrebno je bilo prikupiti 524288 ETH (16384 validatora, ovi brojevi su odlučeni kako bi se obezbedila dovoljna sigurnost i decentralizacija) za lansiranje *Beacon* lanca – blokčejn lanca koji koristi PoS mehanizam konsenzusa. Ovaj lanac je kreiran kako bi se osiguralo da je logika PoS mehanizma održiva pre nego što bi se omogućila na *Ethereum*-ovoj glavnoj mrezi tzv. *mainnet*-u. Uporedo sa ovim lancem postojao je originalni lanac koji koristi PoW mehanizam konsenzusa sve do trenutka spajanja, tzv. *The Merge* događaja, što je zapravo i sledeća faza - faza 1. *Beacon* lanac nije mogao da procesuira transakcije, izvršava pametne ugovore i hostuje decentralizovane aplikacije.

4.1.1. Gasper algoritam

PoS mehanizam konsenzusa koji *Ethereum* 2.0 koristi se oslanja na Gasper algoritam. Gasper algoritam definiše kako se validatori nagrađuju i kažnjavaju, odlučuju koje blokove da prihvate i odbace i koju granu blokčejna da nadograđuju, tj. dodaju nove blokove. Gasper algoritam je dizajniran da zameni energetski intenzivan proces rudarenja sa energetski znatno efikasnijim procesom validacije. U novom sistemu korisnici, da bi postali validatori, moraju uložiti minimalno 32 ETH u pametni ugovor na originalnom *Ethereum* lancu. Zatim se identična količina ETH kreira na *Ethereum* 2.0 lancu i korisnici je mogu iskoristiti da postanu validatori. Bitno je napomenuti da ETH koji je kreiran na *Ethereum* 2.0 mreži se ne može konvertovati nazad u originalni lanac. Alternativno, verifikaciju i validaciju blokova izvršavaće validatori koji su odabrani prema uloženom depozitu. Drugim rečima, moć glasanja svakog validatora će biti određena količinom ETH koju su založili. Takođe, uloženi depozit se može izgubiti ukoliko čvorovi nisu pošteni u predlaganju ili validaciji blokova ili su neaktivni.

U svakom slotu (period u trajanju od 12 sekundi) nasumično se bira validator koji treba da predloži blok. Nasumičnost se postiže korišćenjem algoritma RANDAO koji kombinuje heš vrednost predlagača bloka sa *seed*-om koji se ažurira u svakom slotu. Izbor validatora je fiksiran dve epohe unapred (svaka epoha iznosi 32 slota, tj. 6.4 minute) kao način zaštite od manipulacije *seed*-om. Validatori se stalno dodaju u RANDAO, ali se globalna RANDAO vrednost ažurira samo jednom po epohi [4]. Validatori grupišu transakcije, izvršavaju ih, umotavaju u blok i šalju drugim validatorima. Validatori kada dobiju novi blok ponovo izvršavaju transakcije kako bi se uverili da li se slažu sa predloženom izmenom stanja. Ukoliko je blok validan, dodaju ga u svoju bazu podataka.

4.2. Faza 1

Faza 1 se još naziva i *The Merge* i odigrala se 15. septembra 2022. godine kada je *Beacon* lanac spojen sa *mainnet*-om. Dobijeni lanac izvršavao je PoS koncenzus mehanizam, rudarenje više nije bilo sredstvo za kreiranje novih blokova. Ovo ažuriranje mreže nazvano je Pariz. Svrha spajanja bila je eliminacija PoW algoritma, budući da je jedan lanac (*beacon*) koristio PoS, a drugi lanac (*Mainnet*) PoW. Sveukupno gledano, prelazak na PoS učinio je *Ethereum* znatno efikasnijim i decentralizovanijim – što više korisnika učestvuje u mreži ona postaje bezbednija i decentralizovanija.

Korišćenje PoS algoritma je osnovna komponenta za siguran, ekološki prihvatljiv i skalabilan *Ethereum* koji danas postoji.

4.3. Faza 2

Faza 2 ima za cilj implementaciju šardova. Prvobitno, plan je bio da se na šardovanju poradi pre samog *Merge*-a, kako bi se rešio problem skalabilnosti. Međutim, sa rešenjem za skaliranje drugog sloja, prioriteti su se izmenili, te se faza 2 još nije ni odigrala. Šardovanje je vid particionisanja podataka, gde se velika baza podataka deli na manje kako bi se lakše upravljalo manjim delovima i povećala celokupna efikasnost. Na primeru blokčejna, šardovanje se odnosi na deljenje lanca na više manjih čime se stvara struktura mreže. Ovo doprinosi smanjenju radnog opterećenja validatora koji skladište i upravljaju samo jednim delom mreže umesto celim blokčejnom. Drugi sloj je zajednički naziv za rešenja za skaliranje rukovanjem transakcija van glavne mreže *Ethereum*-a uz korišćenje prednosti glavne mreže. Većina rešenja se odnosi na server ili klaster servera. Transakcije se podnose čvorovima na drugom sloju, umesto direktno na prvi sloj. Glavna ideja koja stoji iza drugog sloja jeste povećanje protoka transakcija, ali bez žrtvovanja decentralizacije i bezbednosti.

5. ISTRAŽIVAČI BLOKOVA

Podaci blokčejna su javno dostupni. Istraživači blokova (engl. *block explorer*) omogućavaju pristup podacima vezanim za transakcije na blokčejnu, uključujući iznos transakcije, njen status, pošiljaoca i primaoca. Podaci koji su dostupni za pregled su podeljeni u dve grupe: podaci izvršavanja i koncenzus podaci. Podaci izvršavanja se odnose na transakcije koje su izvršene u okviru specifičnog bloka ethorg. Koncenzus podaci se odnose sa blokove i validatore koji su ih predložili.

Za pregledanje transakcija i blokova u radu je korišćen *EtherScan* istraživač bloka. Za potrebe kreiranja transakcije preduslov je bio imati novčanik, stoga je iskorištena *MetaMask* brauzer ekstenzija za kreiranje novčanika, a kako bi se dobili ETH i inicirala transakcija iskorišćen je *Sepolia faucet.* Za realizaciju transakcije korišćena je *Ethereum*-ova testna mreža – *Sepolia*.

Nakon uspešne ETH transakcije, na *Etherscan*-u su prikazani njeni podaci. Kako je korišćena *Sepolia* testna mreža, neophodno je bilo koristiti i *Etherscan* namenjen ovoj testnoj mreži. Radi pretrage transakcija koristi se heš same transakcije koji se može pronaći u okviru *MetaMask* novčanika. Nakon unosa heša transakcije, detalji koji su prikazani za transakciju su sam heš transakcije, njen status, broj bloka kojem ona pripada, kada je izvršena, javne adrese primaoca i pošiljaoca, kao i vrednost koja je poslata, gas (jedinica koja meri količinu računarskog napora potrebno za izvršenje operacije na *Ethereum* mreži) i nadoknada za transakciju. Ukoliko transakcija nije bila uspešna, umesto statusa *success/successful* može da se nađe još opcija:

- poruka o greški – *bad instruction/out of gas*
- status na čekanju – transakcija čeka da bude potvrđena/obrađena
- nije pronađena - ili transakcija nije prošla ili još uvek nije prikazana u istraživaču bloka
- vraćena – greška korisnika pametnog ugovora, neophodno je još jednom proveriti detalje transakcije

Moguća je i inspekcija samog bloka kojem data transakcija pripada, ukoliko se klikne na prikazani broj bloka. Uz to, ukoliko se u polje za pretragu unese javna adresa računa, moguće je vršiti inspekciju aktivnosti računa i njegovo stanje. *Etherscan*, pored navedenih primena, ima i mnoge druge, kao što je inspekcija pametnih ugovora (može se pregledati i njihov izvorni kod), nezamenljivih tokena, može se pratiti statistika mreže (*Topstat* stranica), mogu se uključiti notifikacije za praćenje aktivnosti određenog računa/adrese i još mnogo toga.

6. ZAKLJUČAK

U radu su opisane tri faze ažuriranja *Ethereum* mreže. Objašnjen je koncept blokčejna, i uz to su detaljno opisani konsenzus mehanizmi koji mreže *Ethereum* 1.0 i 2.0 koriste. Korišćenjem *MetaMask* novčanika i *Sepolia* testne mreže su izvršene transakcije, a zatim pomoću *Etherscan*-a je izvršen i uvid u detalje same transakcije na blokčejnu.

Ažuriranje *Ethereum* mreže donelo je mnogo prednosti, smanjeni su hardverski zahtevi budući da se više ne koristi hardverski zahtevan PoW konsenzus mehanizam. Iz istog razloga, sada je *Ethereum* više ekološki prihvatljiv jer je smanjena potrošnja električne energije. Još jedna prednost su i niže transakcijske nadoknade, kao i povećanje propusnosti mreže na kojem je ideja i da se ubuduće radi.

7. LITERATURA

[1] Maarten van Steen, Andrew S. Tanenbaum, Distributed Systems, 2018

[2] Imran Bashir, Mastering Blockchain, 2017

[3] Dejan Vujičić, Siniša Ranđić, Blockchain technology, bitcoin, and Ethereum: A brief overview, 2018

[4] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos (pregledano avgusta 2023.)

Kratka biografija:

Jelena Cupać rođena je 03.02.1999. u Somboru. U Sivcu je završila Osnovnu školu „20. oktobar“ 2013. godine kao nosilac Vukove diplome i zvanja Đaka generacije. Iste godine upisuje gimnaziju „Veljko Petrović“ u Somboru, prirodno- matematički smer. Godine 2017. završava gimnaziju kao nosilac Vukove diplome. Nakon završene gimnazije, upisuje Fakultet tehničkih nauka Univerziteta u Novom Sadu, smer Softversko inženjerstvo i informacione tehnologije. Sve ispite polaže i studije završava u roku, 2021. godine. Iste godine, upisuje master studije na Fakultetu tehničkih nauka, smer Elektronsko poslovanje. Sve ispite polaže i studije završava 2023. godine.
kontakt: cupac.r230.2021@uns.ac.rs