Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.738
DOI: https://doi.org/10.24867/30BE52Mijonic

ARHITEKTURA I PERFORMANSE EVM BLOK EKSPLORER-A

ARCHITECTURE AND PERFORMANCE OF EVM BLOCK EXPLORER

Nikola Mijonić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – PRIMENJENE RAČUNARSKE NAUKE I INFORMATIKA

Kratak sadržaj – *Ovaj rad pruža uvid u implementaciju EVM blok pretraživača sa fokusom na arhitekturu i performanse. Rad sadrži opis ključnih pojmova Ethereum platforme kako bi rad bio razumljiviji.*

Ključne reči: *blokčejn, pretraživač, arhitektura, performanse*

Abstract – *This paper provides an insight into the implementation of an EVM block explorer with a focus on architecture and performance. It includes a description of key concepts of the Ethereum platform to make the paper more comprehensible.*

Keywords: *blockchain, explorer, architecture, performance*

1. UVOD

Razumevanje tehnologije lanca blokova [1] kao i njene upotrebne vrednosti zahteva osnovno poznavanje istorije novca i monetarnih sistema. Nepoznavanje materije i finansijska nepismenost često dovode do netačnih zaključaka kao što su osporavanje finansijske vrednosti pojedinih kriptovaluta kao i same upotrebne vrednosti. Postojeći monetarni sistemi su veoma centralizovani što u svojoj osnovi nije dobro jer se javlja problem centralizacije moći i neadekvatnog upravljanja novcem u vidu nekontrolisanog štampanje bez ikakvog pokrića.

Osnovna ideja *Ethereum* [2] mreže je da pruži infrastrukturu za razvoj decentralizovanih aplikacija. Problemi vezani za centralizaciju monetarnih sistema prisutni su i u domenu centralizovanih aplikacija. Cenzure na društvenim mrežama, sprečavanje informisanje u vidu centralizovanih medija, olakšani hakerski napadi usled postojanja centralizovane tačke ispada samo su neki od problema koji bi trebalo da budu rešeni decentralizovanim aplikacijama.

Podaci koji su pohranjeni na *Ethereum* mrežu ne mogu se menjati što ujedno znači da ne postoji mogućnost malverzacije prethodno sačuvanim informacijama. Detaljan opis *Ethereum* mreže može se pronaći u okviru ovog rada. Postajanje podataka nema preveliku vrednost ukoliko ne postoji jednostavan način da se ti podaci pregledaju odnosno čitaju. Upravo to je razlog postojanja blokčejn pretrazivača.

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

Postojanje mogućnosti da se u svakom trenutko može videti svaka tanskacija koja se dogodila na *Ethereum* mreži koja je po svojoj prirodu javna je nešto što je za očekivati. Interesovanja za analizu velike količine podataka je sve veće zbog vrednosti koju te informacije donose. Na istom principu postoji potreba da podaci prisutni u *Ethereum* mreži budu pristupačni.

Kao što se može i pretpostaviti usled mogućnosti monetizacije pretraživača blokčejn mreže nije jednostavno steći uvid u arhitekturu i performanse jednog pretraživača. Motiv za ovaj rad je pružanje uvida u stavke o kojima treba voditi računa pri implementaciji pretraživača EVM mreže kao i potencijalnim optimizacijama kada su performanse u pitanju. U okviru ovog rada može se pronaći detaljan opis postupka implementacije blokčejn pretraživača koji je baziran na *Ethereum* mreži, odnosno podatke dobavlja sa pomenute mreže.

1.1. Primena lanca blokova

Transfer novca između država predstavlja nešto sa čime se mnogi susretnu u nekom trenutku života. Troškovi koji nastaju u jednom takvom procesu ne idu u korist onoga ko šalje ili prima novac. Kada na sve to dodamo vreme potrebno da se transakcija procesuira i procenat koji razni entiteti u tom procesu uzimaju može se zaključiti da tu postoji dosta prostora za promene. Prenos novca upotrebom blokčejn tehnologije može biti izuzetno jeftin i uklanja se problem postojanja graničnih podela na države.

Glasanje o donošenju važnih odluka vrlo često je podložno manipulacijama i nekorektnostima. Ovo je nešto što vrlo jednostavno može da se reši upotrebom tehnologije lanca blokova. Pojedinac može da se identifikuje svojom javno dostupnom adresom i ostavi glas, a da je i dalje pseudo anoniman.

Igrice su u velikom broju slučajeva sastavni deo jednog perioda života muške populacije. Neretko se dešava da se enormne količine vremena utroše na aktivnosti ovog tipa što kod većine u zrelijim dobima uzrokuje osećaj griže savesti usled izgubljenog vremena. Nakon prestanka igranja igrice u većini slučajeva ne postoji nikakva mogućnost ostvarivanja monetarnih dobara. Lanac blokova omogućava čuvanje raznoraznih kolekcija koje se nakon prestanka igranja pojedinih igrica mogu prodati i na taj način se može prihodovati.

2. OPIS KORIŠĆENIH TEHNOLOGIJA I ALATA

2.1. Tehnologije

C# [3] - predstavlja objektno orijentisani programski jezik razvijen od stane Majkrosofta (eng. *Microsoft*). Veliku primenu pronašao u razvoju desktop i veb aplikacija.

ASP .Net Core [4] – predstavlja okvir (eng. Framework) javno dostupnog koda koji je namenjen za ravoj zadnje strane veb aplikacija.

Azurne funkcije (eng. *Azure Functions*) [5] - predstavlja proizvod razvijen od strane Majkrosofta (eng. Microsoft) i pruža mogućnost izvršavanja bez servera (eng. *Serverless*). Svoju primenu pronašle su u situacijama kada imamo kod koji će se izvršavati po potrebi.

React [6] – prestavlja biblioteku razvijenu od straje Fejsbuka (eng. Facebook) koja omogućava razvoj modernih veb aplikacija.

Tajpskript (eng. *TypeScript*) [7] – predstavlja jezik otvorenog koda napravljen kako bi rešio i olakšao programiranje u već postojećem javaskript (eng. *JavaScript*) jeziku.

HTML (eng. *HyperText Markup Language*) [8] – predstavlja opisni jezik namenjen za opis prednje strane veb aplikacije.

CSS (eng. *Cascade Style Sheet*) [9]- predstavlja jezik čijom upotrebom se definiše izgled prethodno kreiranih HTML tagova.

Elastični pretraživač (eng. *Elasticsearch*) [10] - predstavlja distribuirani, *RESTful* pretraživač i analitički motor zasnovan na *Apache Lucene*. Dizajniran je da bude brz, skalabilan i lako proširiv, omogućavajući pretragu, analizu i vizualizaciju ogromnih količina podataka u realnom vremenu.

2.2. Alati

Vižual studio kod (eng. *Visual Studio Code*) [11] - predstavlja kod editor koji je razvijen od strane Majkrosofta (eng. Microsoft).

Vižual studio 2022 (eng. *Visual Studio 2022*) [12] - predstavlja razvojno okruženje razvijeno od strane Majkrosofta (eng. *Microsoft*).

Doker desktop (eng. *Docker Desktop*) [13] – predstavlja aplikaciju koja se na *Windows* operativni sistem instalira u nekoliko jednostavnih koraka. Ovaj alat korišćen je za pokretanje elastičnog pretraživača.

Kibana [14] – predstavlja vizualizacijski alat otvorenog koda koji se koristi za pretragu, analizu i vizualizaciju podataka pohranjenih u *Elasticsearch.*

3. ETERIJUM

Ethereum je globalno decentralizovana računarska infrastruktura koja funkcioniše kao svetski kompjuter. Iz perspektive računarskih nauka *Ethereum* je deterministička mašina stanja sa globalno dostupnim jedinstvenim stanjem i virtuelnom mašinom koja primenjuje promene na to stanje. Praktično gledano, *Ethereum* koristi lanac blokova za sinhronizaciju i skladištenje promena stanja sistema, dok se kriptovaluta *Ether* koristi za merenje i ograničavanje troškova resursa izvršenja.

Sposobnost Eterijuma da izvršava programe u svojoj virtuelnoj mašini, poznatoj kao *Ethereum Virtual Machine* (*EVM*) [15], dok čita i piše podatke u memoriji, čini ga Turing-kompletnim [16] sistemom. To znači da *Ethereum* može izvršavati bilo koji algoritam koji je izvodljiv na Turingovoj mašini, pod uslovom da postoji dovoljno memorije.

Ethereum uvodi mehanizam zvan gas, koji meri i ograničava količinu resursa koje jedan pametni ugovor može potrošiti. Svaka instrukcija u *EVM*-u ima unapred određenu cenu u jedinicama gasa, a kada transakcija pokrene izvršenje pametnog ugovora, mora sadržati određeni iznos gasa koji postavlja gornju granicu za izvršenje.

Transakcija je pojedinačna instrukcija koja je kriptografski potpisana i konstruisana od strane aktera u mreži. Pošiljalac transakcije ne može biti pametan ugovor. Iako se pretpostavlja da će konačni spoljnji akter biti ljudske prirode, za konstrukciju i distribuciju transakcija koriste se softverski alati.

Ethereum novčanik je alat koji omogućava korisnicima da upravljaju svojim sredstvima i interaguju sa *Ethereum* lancem blokova. On čuva privatne ključeve koji su ključni za pristup *Ethereum* adresama i sredstvima, dok se javni ključ povezuje sa adresom na kojoj su sredstva pohranjena. Novčanik omogućava slanje i primanje *ETH*-a i tokena, kao i interakciju sa pametnim ugovorima i decentralizovanim aplikacijama.

Blok je osnovna jedinica podataka u *Ethereum* lancu blokova, koja sadrži informacije o transakcijama i promenama stanja u mreži. Svaki blok sadrži skup transakcija koje su izvršene u određenom vremenskom periodu, zajedno sa meta podacima kao što su vreme kreiranja bloka, referenca na prethodni blok (poznata kao heš prethodnog bloka), i druge podatke neophodne za validaciju i integraciju sa lancem blokova.

Konsenzus mehanizam *Proof of Stake* (*PoS*) [17] u *Ethereum* mreži predstavlja ključnu promenu u načinu na koji se novi blokovi dodaju u mrežu i održava sigurnost mreže. U *PoS* sistemu, umesto da rudari rešavaju složene matematičke probleme kao što je to bio slučaj u *Proof of Work* (*PoW*) [18] sistemu, validatori su odabrani na osnovu količine Eterijuma koju su založili kao garanciju.

4. PRETRAŽIVAČ LANCA BLOKOVA

Pretraživač lanca blokova je sofisticirani alat koji omogućava korisnicima da pretražuju, pregledaju i analiziraju sve podatke unutar mreže. Njegova svrha je pružiti transparentnost, uvid u aktivnosti i informacije koje se odvijaju na mreži, te omogućiti lakše praćenje i razumevanje funkcionalnosti i transakcija unutar mreže.

4.1. Funkcionalnosti

Vrlo često se javlja potreba pregleda poslednjih blokova odnosno transakcija na mreži. Inicijalna stranica implementiranog pretraživača sadrži vizuelni prikaz poslednjih blokova i transakcija na mreži. U okviru trake za navigaciju postoji mogućnost pretrage po sledećem kriterijumima: heš vrednosti ili broju kada je reč o blokovima i transakcijama kao i adresi novčanika. U zavisnosti od rezultata korisnik se preusmerava na

odgovarajući prikaz koji sadrži detalje rezultata pretrage. Manipulacija tržištem kpritovalute je prisutna u velikoj meri zbog toga što tržište i dalje nema dovoljno likvidnost što se koristi od strane pojedinaca koji raspolažu velikim sredstvima. Dešavanja u okviru njihovih novčanika često može ukazati na pravac u kojem će se tržište kretati. Upravo iz ovog razloga implementiran je poseban prikaz koji omogućava praćenje velikih transakcija u prethodnom periodu sa ciljem pružanja mogućnosti adekvatno reagovanja na potencijalne promene na tržištu

4.2. Arhitektura i performanse

Jedan od načina za dobavljanje podataka sa mreže bi bio pokretanje lokalno Eterijum čvora što iziskuje određene hardverske resurse kao i samo održavanje u vidu ažuriranja softvera i tako dalje. Kako bi se izbegli problemi koji se mogu javiti prilikom pokretanja jednog takvog čvora donešena je odluka da se iskoristi eksterni servis pod nazivom *Infura* [19] koji pruža usluge manipulacije podacima raznih mreža uključujući i Eterijum. Podaci dobavljeni sa eksternog servisa čuvaju se u elastičnom pretraživaču (eng. *Elasticsearch*).
Kako bi pretraživač imao mogućnost prikazivanja poslednjih blokova sa mreže neophodan je mehanizam sinhronizacije sa dešavanjima prisutnim na mreži, odnosno neophodno je dobavljati nove blokove i transakcije u okviru njih u lokalnu bazu podataka. Upravo ovaj problem rešen je upotrebom Azurne funkcije (eng *Azure function*) koja pruža mogućnost izvršavanja koda bez servera (eng. *Serverless*).
Kako bi lokalno sačuvani podaci postali dostupni prednjoj stranii aplikacije implementiran je interfejs za programiranje aplikacija (eng. *Application Programming Interface*). Ovaj projekat sadrži biznis logiku celokupne aplikacije.
Sa ciljem poboljšanja korisničkog iskustva kada je reč o performansama donešena je odluka da se za bazu podataka koristi elastični pretraživač. Ova tehnologija optimizovana je za veliki broj zahteva koji čitaju podatke. Kako bi se dodatno unapredile performanse donešena je odluka da se implementirana skladištenje podataka u memoriji. *Redis* je izuzetno brz sa mogućnošću obrade miliona zahteva u sekundi.

5. ZAKLJUČAK

Pretraživač lanca blokova predstavlja ključni alat za omogućavanje transparentnosti i analize podataka u okviru mreža. Ovaj alat omogućava korisnicima, istraživačima, regulatorima i razvojnim timovima da efikasno pregledaju sve transakcije, blokove, pametne ugovore i druge aktivnosti unutar mreže, pružajući uvid u decentralizovane sisteme i njihove procese. Tokom istraživanja u ovom radu, pokazano je da pretraživač lanca blokova nudi širok spektar funkcionalnosti, uključujući praćenje stanja adresa, verifikaciju transakcija i analizu blokova. Pored toga, pretraživač se koristi kao alat za analizu učinka mreže, praćenje aktivnosti u cilju prepoznavanja potencijalnih prevara. Buduća istraživanja i razvoj u oblasti pretraživača lanca blokova treba da se fokusiraju na poboljšanje performansi, uvođenje funkcija za zaštitu privatnosti, kao i na interoperabilnost između različitih mreža.

5.1. Predlozi za dalja usavršavanja

Pretraživač lanca blokova treba da bude intuitivan i jednostavan za korišćenje, kako za tehničke korisnike, tako i za širu publiku. Uvođenje vizuelnih prikaza podataka kao što su grafikoni transakcija, dinamika mreže, ili statistike o založenim sredstvima i validatorima može učiniti pretraživač pristupačnijim i razumljivijim. Personalizovani prikazi, filtriranje transakcija prema specifičnim kriterijumima i prikaz ključnih metrika u realnom vremenu dodatno bi poboljšao korisničko iskustvo.
Sa sve većim brojem decentralizovanih aplikacija na platformama poput Eterijuma, neophodno je da pretraživač pruži detaljniji uvid u rad i stanje pametnih ugovora. Ovo uključuje funkcionalnosti za pregled izvornog koda pametnih ugovora, praćenje interakcija sa ugovorima i analizu izvršenja. Mogućnost da se prati istorija ažuriranja ugovora, kao i uvida u potrošnju gasa i efikasnost ugovora, može biti korisna za programere i korisnike.
Kako broj mreža raste, potreba za interoperabilnošću između njih postaje sve važnija. Pretraživač bi trebalo da omogući praćenje više različitih mreža lanca blokova na jednoj platformi, što bi korisnicima omogućilo uvid u transakcije i blokove na različitim mrežama. To bi moglo uključivati i prikaz mostova između mreža, transakcija, kao i stanja u više lanaca.
Uvođenje opcije za korisnike da ocenjuju ili komentarišu određene transakcije ili pametne ugovore može pomoći u jačanju zajednice i omogućiti korisnicima da lakše identifikuju sumnjive ili pouzdane transakcije i ugovore.
Decentralizovane finansije (eng. *DeFi*) [20] su popularan segment ekosistema. Pretraživač može biti proširen kako bi omogućio uvid u interakcije sa *DeFi* protokolima, uključujući pozajmljivanje sredstava, zalaganje, prikupljanje kamate i slično.
Sa rastućom popularnošću tokena i nezamenljivih tokena (eng. *NFT*) [21], pretraživač može biti unapređen tako da omogući detaljno praćenje ERC-721 standarda. Korisnici bi mogli jednostavno da prate transfere tokena, stanje na adresama koje poseduju određene tokene, i pregledaju informacije o samim tokenima, poput njihove vrednosti, vlasništva i meta podataka za NFT tokene.

6. LITERATURA

[1] Blockchain, https://en.wikipedia.org/wiki/Blockchain
[2] Ethereum, https://ethereum.org/en/
[3] Mahesh Chand, Programming C# for Beginners, Garnet Valley PA. Sept 01, 2014, str. 4-7
[4] Kenneth Yamikani Fukizi, Jason De Oliveira and Michel Bruchet, Learn ASP .NET Core 3, Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK. ISBN 978-1-78961-013-0, str. 13-15

[5] Azurne funkcije, https://learn.microsoft.com/en-us/azure/azure-functions/functions-over
[6] React, https://react.dev/
[7] Tajpskript, https://www.typescriptlang.org/docs/handbook/typescript-from-scratch.html
[8] Jon Duckett, HTML & CSS design and build webistes, John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256, str. 20-24
[9] Jon Duckett, HTML & CSS design and build webistes, John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256, str, 227-233
[10] Elastični pretraživač, https://www.elastic.co/elasticsearch
[11] Vižual studio kod, https://code.visualstudio.com/
[12] Vižual studio 2022, https://visualstudio.microsoft.com/vs/
[13] Doker desktop, https://www.docker.com/products/docker-desktop
[14] Kibana, https://www.elastic.co/kibana
[15] EVM, https://ethereum.org/en/developers/docs/evm/.
[16] Turing kompletan, https://en.wikipedia.org/wiki/Turing_completeness
[17] PoS, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
[18] PoV, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/
[19] Infura, https://www.infura.io/
[20] Decentralizovane finansije, https://www.coinbase.com/learn/crypto-basics/what-is-defi
[21] NFT, https://ethereum.org/en/nft/

7. BIOGRAFIJA

Nikola Mijonić je rođen 03.06.1998. godine u Somboru. Srednju elektrotehničku školu “Mihajlo Pupin” završio u Novom Sadu 2017. godine. Iste godine upisao se na studije primenjenog softverskog inženjerstva Fakulteta tehničkih nauka. Položio je sve ispite predviđene planom i programom. Master studije na programu Elektronsko poslovanje upisao 2021. godine i položio sve ispite.