Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/15BE17Radulovic

IMPLEMENTACIJA KONCEPTA DECENTRALIZOVANIH FINANSIJA ZASNOVANA NA PRIMENI POLKADOT ARHITEKTURE

IMPLEMENTATION OF DECENTRALIZED FINANCE CONCEPT BASED ON THE USE OF POLKADOT ARCHITECTURE

Danijel Radulović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu će biti predstavljeni koncepti blokčejna, decentralizovanih finansija i Polkadot blokčejn arhitekture. Biće opisana i konkretna implementacija koncepta decentralizovanih finansija zasnovana na primeni arhitekture Polkadot paralelnog lanca.*

Ključne reči: *distribuirani sistemi, blokčejn, decentralizovane finansije, Polkadot*

Abstract – *In this paper, the concepts of blockchain, decentralized finance and Polkadot blockchain architecture will be presented. The concrete implementation of the concept of Decentralized Finance based on the use of the Polkadot parallel chain architecture will also be described.*

Keywords: *distributed systems, blockchain, Decentralized Finance, Polkadot*

1. UVOD

U prošlosti je bilo mnogo pokušaja kreiranja digitalnog novca, ali su ti pokušaji uvek bili bezuspešni. Glavna prepreka kreiranja digitalnog novca je nedostatak poverenja. Ako bi digitalni novac postojao, kako osigurati da emitent digitalnog novca neće sebi dodeliti milion novčanih jedinica ili prisvojiti odnosno ukrasti digitalni novac za sebe. *Bitcoin*, jedna od najpoznatijih digitalnih kriptovaluta je kreirana na način da reši problem nepoverenja koristeći posebnu bazu podataka, koja je nazvana blokčejn.

Kako se blokčejn tehnologija razvijala, ideja digitalnog novca je konstantno evoluirala i donela novi koncept finansijskog sistema, tzv. decentralizovane finansije (engl. *DeFi*). Decentralizovane finansije se, kao globalni otvoren finansijski sistem, nameću kao alternativa tradicionalnom bankarskom sistemu. Izrada konkretne implementacija *DeFi* rešenja na *Polkadot* blokčejn arhitekturi će biti tema ovog rada.

2. TEORIJSKE OSNOVE BLOKČEJNA I DECENTRALIZOVANIH FINANSIJA

U ovom poglavlju, biće opisani koncepti koji čine teorijske osnove blokčejn tehnologije, počevši od osobina distribuiranih sistema do komponenata koje sačinjavaju jedan blokčejn sistem.

Takođe, biće obrađena i tema decentralizovanih finansija, koje se sve više ističu kao alternativa tradicionalnim bankarskim sistemima.

2.1. Blokčejn

Razumevanje distribuiranih sistema je od suštinskog značaja za razumevanje blokčejna, jer je blokčejn u svojoj osnovi distrubiran sistem. Tačnije, to je decentralizovani distribuirani sistem [1].

2.1.1. Distribuirani sistemi

Distribuirani sistem je skup autonomnih računara koji iz perspektive korisnika izgledaju kao jedan koherentan sistem. Ova definicija obuhvata dve glavne osobine distribuiranih sistema. Prva osobina ističe da je distribuirani sistem skup računara, od kojih svaki može da se ponaša nezavisno od ostalih. Druga osobina ističe da bi, iz perspektive korisnika, distribuiran sistem trebalo da deluje kao jedinstven sistem, tako da korisnici nisu svesni postojanja autonomnih računara [2].

S obzirom na prethodnu definiciju, distribuirani sistemi predstavljaju računarsku paradigmu, u kojoj dva ili više čvorova rade međusobno na koordiniran način radi postizanja zajedničkog ishoda, a da su modelovani na takav način da ih krajnji korisnici vide kao jedinstvenu logičku platformu [1].

Računarske jedinice, koje se češće nazivaju čvorovima (engl. *node*), mogu biti i hardverski uređaji i softverski procesi. Svi čvorovi su sposobni da šalju i primaju poruke između sebe. Čvorovi mogu biti ispravni, neispravni i maliciozni i mogu imati svoju memoriju i procesor. Glavni izazov u dizajnu distribuiranih sistema je koordinacija između čvorova i tolerancija na otkaze. Ako neki od čvorova postanu neispravni ili se mrežne veze prekinu, distribuirani sistem bi trebao tolerisati i nastaviti da radi bez smetnji, kako bi se postigao željeni rezultat.

Ovo je područje aktivnog istraživanja dugi niz godina i predloženo je nekoliko algoritama i mehanizama za prevazilaženje ovih problema.

Na osnovu dosadašnjeg opisa i objašnjenja vezanih za funkcionisanje distribuiranih sistema, mogu se izdvojiti njihove tri glavne karaksteristike:

- Konkurentnost komponenti – U distribuiranom sistemu je dozvoljeno da više klijenata istovremeno pristupi istom resursu, tako da i čvorovi mogu da izvršavaju više poslova istovremeno.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dušan Gajić, vanredni profesor.

- Nepostojanje globalnog sata – U distribuiranom sistemu ne postoji globalno vreme, tj. nisu svi satovi u sistemu sinhronizovani. Postoje algoritmi za sinhronizaciju, poput Berkli algoritma, koji skenira povremeno vrednost svih satova u sistemu, izračunava srednju vrednost i obaveštava sve članove o novom vremenu. S obzirom da često nije važno kada se događaj tačno desio, nego je bitan redosled događaja, uvodi se koncept logičkih satova, relacije desilo-se-pre i vremenskih otisaka.
- Nezavisan otkaz komponenti – Otkaz pojedinačnih komponenti neće uticati na rad sistema.

2.1.2. Komponente blokčejn sistema

Blokčejn je, u svom jezgru, *peer-to-peer* distribuirana glavna knjiga, koja je kriptografski sigurna, pri čemu se u nju može samo dodavati, ne može se izmeniti (izuzetno teško se menja) i ažurira se samo putem konsenzusa ili dogovora između *peer*-ova [1].

Važan pojam za objašnjenje ove definicije je pojam glavne knjige (engl. *ledger*). Glavna knjiga služi za beleženje i sumiranje ekonomskih transakcija. U glavnu knjigu se upisuju transakcije zajedno sa vremenskom oznakom, tako da u njoj postoji nedvosmislen skup svih transakcija u sistemu. Kada se na glavnu knjigu doda princip distribuiranosti, dolazi se do distribuirane glavne knjige, gde su podaci raspoređeni na više fizičkih mašina. Distribuirana glavna knjiga ili tehnologija distribuirane glavne knjige je vrsta distribuirane baze podataka koja pretpostavlja moguće prisustvo malicioznih korisnika (čvorova).

Za razliku od centralizovane glavne knjige koja obično ima centralizovano telo, koje vodi računa o validnosti glavne knjige, kod distribuirane glavne knjige svaki čvor može da upiše novu transakciju i zatim ostali čvorovi glasaju kroz konsenzus algoritam o tome koja kopija je validna. U trenutku kada je konsenzus postignut, svi čvorovi upisuju validnu verziju glavne knjige.

Blokčejn, kao struktura podataka, predstavlja lanac povezanih blokova. Blok predstavlja izbor transakcija zajedno povezanih radi njihove logičke organizacije. Sastoji se od transakcija i njegova veličina je promenljiva u zavisnosti od vrste i dizajna blokčejna koji se koristi. Svaki blok sadrži referencu na prethodni blok, osim ako nije u pitanju blok geneze. Blok geneze je prvi blok u blokčejnu, koji je postavljen kad je blokčejn pokrenut [1].

2.2. Decentralizovane finansije

Decentralizovane finansije (engl. skraćenica *DeFi*), u svojoj osnovnoj formi, predstavljaju sistem pomoću kojeg finansijski proizvodi postaju dostupni na javnoj decentralizovanoj blokčejn mreži, čineći ih otvorenim za svakoga, bez učešća posrednika, poput banaka i brokera. Za razliku od bankovnog ili brokerskog računa, lični dokument, broj socijalnog osiguranja ili dokaz adrese nisu potrebni za upotrebu *DeFi*-ja [3].

Preciznije, *DeFi* se odnosi na sistem pomoću kojeg softver napisan na blokčejnu omogućava kupcima, prodavcima, zajmodavcima i zajmoprimcima *peer-to-peer* interakciju sa striktno softverskim posrednikom, a ne sa kompanijom ili institucijom koja omogućava transakciju [3].

DeFi je otvoren i globalni finansijski sistem izgrađen za doba Interneta – alternativa sistemu koji je neproziran, strogo kontrolisan i koji zajedno drže više decenija stara infrastruktura i procesi. Omogućava korisnicima kontrolu i pregled nad svojim novcem, takođe omogućava izloženost globalnim tržištima i alternative lokalnoj valuti ili bankovnim opcijama. *DeFi* proizvodi otvaraju finansijske usluge svakome ko ima vezu ka Internetu i ceo sistem je u vlasništvu korisnika [4].

Većina *DeFi* aplikacija izgrađena na vrhu *Ethereum* mreže, druge po veličini svetske platforme za kriptovalute, koja se izdvaja od *Bitcoin*-a po tome što je lakše koristiti za izgradnju drugih vrsta decentralizovanih aplikacija, od jednostavnih transakcija.

Složenije slučajeve finansijske upotrebe je čak istakao i tvorac *Ethereum*-a, Vitalik Buterin, još 2013. godine u originalnom belom papiru *Ethereum*-a. Razlog tome su *Ethereum*-ovi pametni ugovori koji automatski izvršavaju transakcije ako su željeni uslovi ispunjeni, samim tim nude i mnogo više fleksibilnosti. Programski jezik *Solidity* je posebno dizajniran za kreiranje takvih pametnih ugovora.

U Tabeli 1 prikazano je poređenje između decentralizovanih i tradicionalnih finansija.

Tabela 1. *Poređenje DeFi-ja i tradicionalnih finansija*

Decentralizovane finansije	**Tradicionalne finansije**
Korisnik drži svoj novac	Korisnikov novac je u vlasništvu kompanije
Korisnik kontroliše kretanje i potrošnju svog novca	Potrebno je poverenje u kompanije da neće loše upravljati korisnikovim novcem, poput pozajmljivanja rizičnim zajmoprimcima
Transfer sredstava se vrši u nekoliko sekundi ili minuta	Plaćanja mogu trajati danima zbog manuelne obrade
Transakciona aktivnost je pseudoanonimna	Finansijska aktivnost je čvrsto povezana sa korisnikovim identitetom
DeFi je otvoren za svakoga	Korisnik se mora prijaviti za korišćenje finansijskih usluga
Tržište je otvoreno uvek	Tržišta se zatvaraju jer je zaposlenima potrebna pauza
Zasnovano na transparentnosti – svako može pogledati podatke o proizvodu i pregledati kako sistem funkcioniše	Finansijske institucije su „zatvorene knjige“ – ne možete tražiti da vidite njihovu istoriju kredita, zapis o upravljanju imovinom itd

U najpoznatije *DeFi* aplikacije spadaju [5]:

- Decentralizovane menjačnice (engl. skraćenica *DEX*) – Pomažu korisnicima da razmene valute za druge valute, bilo da su to američki dolari za *Bitcoin* ili *Bitcoin* za *Ethereum*. Trenutno su veoma popularna vrsta menjačnica, koja direktno povezuje korisnike kako bi mogli međusobno da trguju kriptovalutama bez posrednika, kojem bi poverili svoj novac.
- Stabilni novčići (engl. *Stablecoins*) – Kriptovalute koje su vezane za imovinu izvan kriptovaluta (npr. dolar ili evro), radi stabilizacije cene.
- Platforme za pozajmljivanje – Ove platforme koriste pametne ugovore umesto posrednika poput banaka koje upravljaju kreditiranjem.
- „Obmotan“ *Bitcoin* (engl. skraćenica *WBTC*) – Način slanja bitkoina na *Ethereum* mrežu, pružaju mogućnost korisnicima da zarađuju kamatu na *Bitcoin*-u, koji pozajmljuju putem gorenavedenih decentralizovanih platformi za pozamljivanje.
- Tržišta predikcije – Omogućavaju klađenje na ishod budućih događaja poput izbora.

Decentralizovane finansije su još u početnoj fazi svoje evolucije. Ukupna vrednost zaključana u *DeFi* pametnim ugovorima iznosi više od 84 milijarde dolara zaključno sa avgustom ove godine. Ukupna zaključana vrednost se računa množenjem broja tokena u protokolu sa njihovom vrednošću, izraženom u dolarima.

DeFi ekosistem je i dalje prepun infrastrukturnih grešaka, hakova i prevara. Jedna od najčešćih prevara predstavlja „povlačenje tepiha“ (engl. *rug pull*) , u kojima hakeri iscrpljuju sredstva iz protokola i onemogućavaju trgovanje investitorima. Takođe, postoje i dobro uspostavljeni protokoli, koji mogu značajno smanjiti rizik.

Otvorena i distribuirana priroda decentralizovanog finansijskog ekosistema može predstavljati i problem postojećim finansijskim propisima. Trenutni zakoni izgrađeni su na osnovu ideje o odvojenim finansijskim jurisdikcijama, od kojih svaka ima svoj skup zakona i pravila. *DeFi*-jev raspon transakcija bez granica predstavlja važna pitanja za ovu vrstu propisa, npr. ko je kriv za finansijski zločin, koji se događa preko granica, protokola i *DeFi* aplikacija [4].

Pametni ugovori su još jedno područje zabrinutosti za *DeFi* regulativu. Pored uspeha *Bitcoin*-a, *DeFi* je najjasniji primer teze „kod je zakon“, gde zakon predstavlja skup pravila, napisanih i primenjenih kroz nepromenljivi kod. S obzirom na to, greške su i dalje vrlo česte. Pametni ugovori su moćni, ali se ne mogu promeniti kada se pravila unesu u protokol, što često čini greške trajnim.

3. *POLKADOT* BLOKČEJN

Polkadot predstavlja mrežni protokol koji omogućava prenos proizvoljnih podataka, ne samo tokena, preko više blokčejn mreža. To znači da je *Polkadot* pravo okruženje za implementaciju interoperabilnosti između više različitih blokčejn mreža. *Polkadot* omogućava prenos podataka preko javnih, otvorenih i blokčejn mreža bez kontrole prava pristupa pa do privatnih mreža i blokčejn mreža sa kontrolom prava pristupa [6].

Tvorac *Polkadot*-a i suosnivač *Ethereum*-a, Gejvin Vud, je u belom papiru, opisao *Polkadot* kao skalabilni heterogeni višelančani blokčejn. Ovo znači da za razliku od prethodnih implementacija blokčejna, koji su se fokusirali na obezbeđivanje jedinstvenog lanca različitih stepena opštosti nad potencijalnim primenama, *Polkadot* je dizajniran tako da ne pruža nikakvu inherentnu funkcionalnost aplikacije, već pruža osnovni relejni lanac na kome veliki broj validnih i globalno koherentnih dinamičkih struktura podataka mogu biti korišćene rame uz rame.

Polkadot omogućava internet na kojem nezavisni blokčejnovi mogu razmenjivati informacije i transakcije preko relejnog lanca *Polkadot* mreže. Olakšava stvaranje i povezivanje decentralizovanih aplikacija, usluga i institucija.

Osnovne komponente od kojih je sačinjena *Polkadot* arhitektura su [7]:

- Paralelne niti (engl. *parathreads*) – Ideja za paralelne lance da privremeno (na nivou bloka) učestvuju u bezbednosti mreže, bez potrebe da iznajmljuju namensko mesto za paralelni lanac. Ovo se postiže ekonomičnim deljenjem resursa mesta za paralelni lanac među brojnim konkurentima, tj. paralenim nitima.
- Paralelni lanci (engl. *parachains*) – Struktura podataka specifična za aplikaciju, koja je globalno koherentna i koju mogu validirati validatori relejnog lanca. Najčešće paralelni lanci imaju oblik blokčejna, ali nema posebne potrebe za tim, tako da ne moraju biti u tom obliku. Zbog svoje paralelne prirode oni su u stanju da paralelizuju obradu transakcija i postignu skalabilnost *Polkadot* sistema. Takođe, učestvuju u bezbednosti cele mreže i mogu da komuniciraju sa drugim paralelnim lancima putem *XCMP*-a .
- Relejni lanac (engl. *relay chain*) – Centralni lanac *Polkadot*-a. Svi validatori *Polkadot* mreže zalažu svoja sredstva u relejni lanac u vidu *DOT* tokena. Relejni lanac sastoji se od relativno malog broja vrsta transakcija, kao što su interakcija sa mehanizmom upravljanja (engl. *governance*), aukcije za paralelne lance i učešće u postizanju konsenzusa. Glavna odgovornost je da koordinira sistem u celini, uključujući paralelne lance. Drugi specifični poslovi delegirani su paralelnim lancima, koji imaju različite implementacije i karakteristike
- Mostovi (engl. *bridges*) - Omogućavaju paralelnim lancima i paralelnim nitima da se povezuju i komuniciraju sa spoljnim mrežama poput *Ethereum*-a i *Bitcoin*-a.

4. KORIŠĆENE TEHNOLOGIJE

U implementaciji *DeFi* rešenja vezanog za ovaj rad, korišćeno je programsko okruženje *Substrate* i njegova integracija sa *Polkadot-JS* bibliotekom.

Ključni koncepti *Substrate*-a su *runtime*, *extrinsic*, apstrakcije naloga (engl. *Account Abstractions*), „bazen“

transakcija (engl. *Transaction Pool*), ključevi sesije (engl. *Session Keys*), težine transakcija (engl. *Transaction Weights*) i karakteristike van lanca (engl. *Off-chain features*). *Runtime* blokčejna je poslovna logika koja definiše njegovo ponašanje. U *Substrate* blokčejnovima, runtime se naziva "funkcija prelaska stanja", tu programeri definišu stavke skladišta koje se koriste za predstavljanje stanja blokčejna, kao i funkcije koje omogućavaju korisnicima blokčejna da unesu promene u to stanje [8]. Osnovna kodna baza *Substrate*-a isporučuje se sa *FRAME*-om, *Parity*-jevim sistemom za razvoj Substrate runtime-a, koji se koristi za lance poput *Kusama*-e i *Polkadot*-a. *FRAME* definiše dodatne primitive za *runtime* i pruža okruženje, koje olakšava konstrukciju *runtime*-a sastavljanjem modula, koji se nazivaju palete (engl. *pallets*). Svaka paleta obuhvata logiku specifičnu za domen, koja je izražena kao skup stavki skladišta, događaja, grešaka i otpremljivih funkcija, koje korisnici mogu pozivati [8].
Extrinsic-a predstavlja podatak koji dolazi izvan lanca, tj. mreže i uključen je u blok. *Extrinsic*-e se dele u tri kategorije: inherentne, potpisane i nepotpisane transakcije. *Extrinsic*-e su povezane zajedno u blok, kao niz koji se izvršava u redosledu definisanja extrinsic-e u toku vremena izvršavanja. Potpisane transakcije odgovaraju konceptu transakcije u *Ethereum*-u ili *Bitcoin*-u.
Polkadot-JS API je biblioteka interfejsa za komunkaciju sa *Polkadot* i *Substrate* čvorovima. *API* pruža mogućnost programerima aplikacija da postavljaju upite čvoru i stupaju u interakciju sa *Polkadot* i *Substrate* lancima, koristeći *Javascript*.

5. REŠENJE

Data implementacija *DeFi* rešenja predstavlja prototip *DeFi* platforme za pozajmljivanje sredstava, koja ima ulogu banke i praktično omogućava klasične tradicionalne usluge štednje i podizanja kredita. Implementacija ideje je zasnovana na konceptima *Polkadot* paralelnog lanca. Za izradu rešenja, kao osnova je iskorišćen već kreirani šablon *Substrate* čvora. *Substrate* projekat, kao što je ovaj, sastoji se od brojnih komponenti, koje su logički raspoređene u nekoliko direktorijuma. U *runtime* direktorijumu se nalazi datoteka za podešavanje i konfiguraciju *runtime*-a, definisanje vrednosti inicijalnih parametara paleta, kao i definisanje *RPC* metoda, koje korisnik može pozivati, kako bi dobio informacije o trenutnom stanju sistema. Konkretna *DeFi* paleta, koja predstavlja priloženo rešenje, sadrži pet *RPC* metoda: metodu za dobijanje trenutnog balansa korisnika sa obračunatom depozit kamatom, metodu koja vraća trenutni dug naloga sa obračunatom kamatom za pozajmicu, metodu koja vraća dozvoljenu visinu pozajmice za određenog korisnika, kao i metode za dobijanje vrednosti godišnje kamate na depozit i pozajmicu.
Od funkcionalnosti, tj. *extrinsic* metoda koje menjaju stanje sistema, podržan je depozit sredstava i stavljanje na štednju, povlačenje sredstava, uzimanje pozajmice i otplata duga.
U cilju poboljšanja ovog rešenja, jasno se nameće ideja uvođenja još kriptovaluta u kojima bi se mogle koristiti navedene usluge. Takođe, jedno od unapređenja bi moglo biti i uvođenje promenljivih kamata, kao i usluge brze pozajmice (engl. *flash loan*) koja predstavlja uzimanje i vraćanje pozajmice u okviru jednog bloka, što je nemoguće postići u tradicionalnom sistemu. Navedena poboljšanja predstavljaju, trenutno, sastavni deo svake veće *DeFi* platforme u blokčejn svetu.

6. ZAKLJUČAK

Blokčejn, kao tehnologija budućnosti, koja je pronašla svoje mesto u javnosti, zahvaljujući ideji digitalnog novca i kriptovaluta je započela revoluciju, od koje se očekuje da će se razvijati eksponencijalno. Širom sveta vlada veliko interesovanje za blokčejn tehnologijom od strane istraživača i raznih organizacija, što utiče veoma pozitivno na njen potencijal, konstantno donoseći nove koncepte i usavršavanje postojećih.
Decentralizovane finansije predstavljaju jednu od najbrže rastućih oblasti u blokčejn industriji. Centralizovani sistemi i ljudski faktori mogu ograničiti brzinu i sofisticiranost transakcija, dok korisnicima nude manje direktne kontrole nad novcem. Mnogi veruju da različiti *DeFi* projekti imaju veliki potencijal, privlačeći mnoštvo novih korisnika, čineći finansijske aplikacije inkluzivnije i otvorenije za one koji tradicionalno nemaju pristup takvim platformama.

LITERATURA

[1] I. Bashir, Mastering Blockchain, Packt, 2017.
[2] M. v. Steen i A. S. Tanenbaum, Distributed Systems, Prentice-Hall, 2017.
[3] R. Sharma, „Decentralized Finance (DeFi) Definition,“ 24.03.2021. [Na mreži]. Available: https://www.investopedia.com/decentralized-finance-defi-5113835 [Poslednji pristup 08.09.2021.]
[4] „Decentralized finance (DeFi),“ [Na mreži]. Available: https://ethereum.org/en/defi/ [Poslednji pristup 08.09.2021.]
[5] A. Hertig, „What Is DeFi?,“ 18.09.2020. [Na mreži]. Available:https://www.coindesk.com/tech/2020/09/18/what-is-defi/ [Poslednji pristup 08.09.2021.]
[6] „Polkadot - Technology,“ [Na mreži]. Available: https://polkadot.network/technology/ [Poslednji pristup 08.09.2021.]
[7] „Polkadot Wiki,“ [Na mreži]. Available: https://wiki.polkadot.network/ [Poslednji pristup 08.09.2021.]
[8] „Substrate Developer Hub - Knowledge Base,“ [Na mreži]. Available: https://substrate.dev/docs/en/ [Poslednji pristup 08.09.2021.]

Kratka biografija:

Danijel Radulović rođen je u Štutgartu, Republika Nemačka, 17. februara 1998. godine. Osnovne akademske studije je upisao na Fakultetu tehničkih nauka Univerziteta u Novom Sadu 2016. godine. Diplomirao je 2020. godine.
Kontakt: master.daca09@gmail.com