Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 007:004.056
DOI: https://doi.org/10.24867/19BE07Bartulov

IMPLEMENTACIJA DECENTRALIZOVANIH FINANSIJSKIH APLIKACIJA NA ETHEREUM PLATFORMI

IMPLEMENTATION OF DECENTRALIZED FINANCIAL APPLICATIONS USING THE ETHEREUM PLATFORM

Marina Bartulov, *Fakultet tehničkih nauka, Novi Sad*

Oblast – RAČUNARSTVO I AUTOMATIKA

Kratak sadržaj – *U ovom radu je opisana implementacija koncepta decentralizovanih finansija na Ethereum platformi u vidu aplikacije za štednju i uzimanje pozajmica. Objašnjene su osnove blockchain tehnologije, sa fokusom na Ethereum. Objašnjen je pojam decentralizovanih finansija i koje probleme rešavaju.*

Ključne reči: *blockchain, Ethereum platforma, pametni ugovori, decentralizovane finansije*

Abstract – *This paper presents an implementation of the concept of Decentralized Finance on the Ethereum platform in the form of an application for lending and borrowing. It explains the basics of blockchain technology, with a focus on Ethereum. It also explains the concept of Decentralized Finance and which problems it solves.*

Keywords: *blockchain, Ethereum platform, smart contracts, decentralized finance*

1. UVOD

Blockchain tehnologija u potpunosti menja način na koji web funkcioniše i njenom pojavom mnoge grane ljudske delatnosti menjaju načine poslovanja i okreću se ka decentralizovanim rešenjima. Jedna od tih oblasti su i finansije. U ovom radu će biti objašenja blockchain tehnologija sa fokusom na Ethereum platfomu i njen uticaj na finansije.

2. BLOCKCHAIN

Da bi se razumeo blockchain potrebno je prvo objasniti šta je to tehnologija distribuirane glavne knjige (eng. *Distributed Ledger Technology - DLT*) i na koji je način povezana sa blockchain-om.

DLT sistemi se mogu definisati kao tip ili podskup distribuiranih sistema [1]. Distribuirani sistemi su računarska paradigma gde dva ili više čvorova koordinisano rade jedni sa drugima kako bi postigli zajednički rezultat. Oni su modelovani tako da ih krajnji korisnici vide kao jednu logičku celinu. Čvor se može definisati kao individualni učesnik u distribuiranom sistemu [2].

DLT sistem predstavlja sistem elektronskih zapisa koji omogućava nezavisnim entitetima da ostvare konsenzus oko deljene „glavne knjige“ (eng. *ledger*) - bez oslanjanja na centralnog koordinatora da obezbedi pouzdanu verziju zapisa. DLT sistemi su dizajnirani da budu sposobni da rade u neprijateljskom (eng. *adversarial*) okruženju, koje je okarakterisano prisustvom malicioznih učesnika u sistemu ili mreži, koji kompromituju sistem koristeći ga na načine za koje nije namenjen. DLT sistemi predstavljaju „konsenzus mašine“, odnosno višeučesničke sisteme u kome učesnici postižu dogovor nad skupom deljenih, validnih podataka, u odsustvu centralnog koordinatora [1].

DLT se odnosi na nov pristup čuvanja i deljenja podataka po mnogobrojnim skladištima podataka (eng. *ledgers*), koji sadrže iste podatke i kolektivno ih održava i kontroliše distribuirana mreža računarskih servera, koji se zovu čvorovi. Blockchain predstavlja poseban tip DLT-a, koji koristi kriptografske i algoritamske metode da kreira i verifikuje stalno rastuću strukturu podataka koja ima oblik lanca blokova sa transakcijama - blockchain - koji vrši funkciju *ledger*-a. Blockchain je određeni mehanizam ili struktura podataka koja koristi kriptografiju ili algoritme da zapisuje podatke na način da ne mogu biti promenjeni [3].

Blockchain je tip baze podataka koja je replicirana po mreži ravnopravnih, nezavisnih učesnika (eng. *peer-to-peer*). Učesnici u mreži postižu konsenzus o promenama stanja deljene baze podataka (tj. transakcijama između učesnika) bez potrebe da veruju u integritet bilo kog učesnika u mreži. Dogovor između učesnika blockchain mreže oko stanja baze podataka se postiže kroz konsenzus mehanizam koji osigurava da svi učesnici imaju isti pogled na deljenu bazu podataka. Kombinacija konsenzus mehanizma sa specifičnom strukturom podataka dozvoljava blockchain-u da reši problem „duplog trošenja“ (mogućnost da se isti digitalni fajl kopira i prenese više puta) bez potrebe za centralizovanom stranom ili centralizovanom glavnom knjigom (eng. *ledger*) koja sprečava korisnike da kopiraju i pošalju isti digitalni fajl dva puta. Blockchain omogućava prenos digitalnih fajlova bez oslanjanja na centralni autoritet. Eliminacija centralnog autoriteta omogućava učesnicima da nezavisno verifikuju da je sadržaj baze podataka koji oni vide u određenom trenutku konzistentan sa onim što vide ostali učesnici. Upravo ta sposobnost učesnika blockchain mreže da nezavisno verifikuju integritet deljenje baze podataka bez oslonca na treću stranu kojoj moraju da veruju je jedna od glavnih vrednosti blockchain-a i razloga za njegovo korišćenje [4].

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

3. ETHEREUM

Ethereum se često opisuje kao „svetski računar“ i predstavlja decentralizovanu računarsku infrastrukturu otvorenog koda koja izvršava programe koji se zovu pametni ugovori. Koristi blockchain za sinhronizaciju i skladištenje promena stanja sistema, zajedno sa kriptovalutom koja se zove ether, koja meri i ograničava troškove resursa za izvršavanje [5].

Svrha i struktura Ethereum-a se znatno razlikuje od blockchain-ova koji su mu prethodili, uključujući i Bitcoin. Svrha Ethereum-a nije da primarno bude mreža za plaćanje digitalnom valutom, nego je on dizajniran da bude programabilni blockchain opšte namene koji pokreće virtuelnu mašinu sposobnu da izvršava kod proizvoljne kompleksnosti. Ether (ETH) je namenjen da bude valuta sa upotrebnom vrednošću (eng. *utility currency*) koja se koristi da bi se platila upotreba Ethereum platforme kao svetskog računara [5].

Namena Ethereum-a je da obezbedi blockchain sa ugrađenim Tjuring kompletnim (eng. *Turing complete*) programskim jezikom koji se može koristiti za kreiranje „ugovora“ koji mogu biti korišćeni za kodiranje proizvoljnih funkcija promene stanja [6].

Ethereum je distribuirana mašina stanja koja prati tranzicije stanja skladišta podataka opšte namene. Ethereum ima memoriju koja skladišti i programski kod i podatke, i koristi Ethereum blockchain da prati kako se ta memorija menja tokom vremena. Ethereum može da učita programski kod u njegovu mašinu stanja i pokrene taj kod, a zatim sačuva rezultirajuće promene stanja na njegov blockchain. Promene stanja Ethereum-a su upravljane pravilima konsenzusa i njegovo stanje je globalno distribuirano [5].

3.1. Pametni ugovori

Pametni ugovor (eng. *smart contract*) je izvršivi programski kod koji se izvršava na blockchain-u kako bi omogućio, izvršio i primenio uslove sporazuma. Glavni cilj pametnog ugovora je da automatski izvrši uslove sporazuma kada su specifični uslovi zadovoljeni. Za razlika od tradicionalnih sistema, pametni ugovori ne zahtevaju poverljivu treću stranu da primeni i izvrši uslove sporazuma. Pametni ugovor ima balans računa (eng. *account balance*), privatno skladište i izvršni kod. Stanje ugovora obuhvata skladište i balans ugovora. Stanje se skladišti na blockchain-u i ažurira svaki put kada se ugovor pozove [7].

U kontekstu Ethereum-a termin „pametni ugovori“ se odnosi na nepromenljive (eng. *immutable*) računarske programe koji se izvršavaju deterministički u kontekstu Ethereum virtuelne mašine (EVM) kao dela Ethereum mrežnog protokola, tj. na decentralizovanom Ethereum svetskom računaru [5].

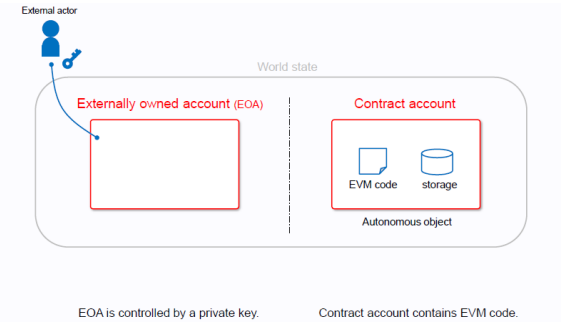
Pametni ugovori se tipično pišu u jeziku visokog nivoa, kao što je Solidity. Ali da bi se mogli izvršiti, moraju biti kompajlirani u bajtkod niskog nivoa koji se izvršava na EVM-u [5].

3.2. Stanje i računi na Ethereum-u

Ethereum stanje se sastoji od objekata koji se zovu računi [10]. Račun predstavlja mapiranje između adrese računa i stanja računa [8].

U Ethereum-u postoje dva tipa računa (eng. *accounts*) (Slika 1) [5]:

1) Eksterno posedovani računi (eng. *externally owned account - EOA*)
2) Računi ugovora (eng. *contract account - CA*)



Slika 1. *Tipovi računa na ethereumu* [8]

Eksterno posedovani računi su oni računi koji imaju privatni ključ, a samim tim i kontrolu nad pristupom sredstvima i ugovorima. EOA kontrolišu korisnici, često putem softvera kao što su novčanici [5]. Ovi računi imaju prazan EVM kod vezan za njih [9].

Račun ugovora ima programski kod pametnog ugovora. Ovakav račun nema privatni ključ i posedovan je i kontrolisan od strane logike koga pametnog ugovora [5]. Ovi računi imaju popunjen EVM kod vezan za njih i kao takvi reprezentuju autonomne objekte (eng. *Autonomous Object*), koji imaju adresu i račun vezan za nju; račun će imati za njega vezan popunjen EVM kod i skladište stanja (eng. *Storage State*) tog računa [9].

3.3 Ethereum virtuelna mašina (EVM)

EVM je deo Ethereum-a koja obavlja isporučivanje pametnih ugovora i njihovo izvršavanje. Na visokom nivou, EVM, koja se izvršava na Ethereum blockchain-u, se može zamisliti kao globalno decentralizovan računar koji sadrži milione izvršivih objekata, svaki sa svojim permanentnim skladištem podataka [5].

To je kvazi potpuna Tjuringova mašina; kvazi dolazi od činjenice da je računanje ograničeno kroz parametar, gas, koji ograničava ukupnu odrađenu količinu računanja [9]. Svi procesi izvršavanja su ograničeni na konačan broj koraka računanja količinom dostupnog gasa za svako izvršavanje pametnog ugovora [5].

3.4 Konsenzus mehanizam

Ethereum trenutno koristi PoW (*Proof-of-Work*) konsenzus mehanizam [10]. Međutim, u procesu je prelaska na PoS (*Proof-of-Stake*) konsenzus mehanizam, koji zahteva da korisnici ulože svoj ETH kako bi postali validatori u mreži. Na taj način oni postaju odgovorni za redanje transakcija i kreiranje novih blokova tako da se svi čvorovi mogu dogovoriti oko stanja mreže [11].

3.5 ERC20 tokeni

Tokeni koji su upravljani na blockchain-u predstavljaju blockchain bazirane apstrakcije koje se mogu posedovati i koje reprezentuju imovinu (eng. *assets*), valutu, prava pristupa i sl. Tokeni su zamenljivi (eng. *fungible*) ako se svaka jedinica tokena može zameniti sa drugom bez bilo kakve razlike u njenoj vrednosti ili funkciji. Nezamenljivi tokeni (eng. *non-fungible*) su tokeni gde svaki reprezentuje jedinstveni opipljivi ili neopipljivi predmet i

prema tome nisu zamenljivi. ERC20 standard je standard za *fungible* tokene i on definiše interfejs za pametne ugovore koji implementiraju token, tako da se svakom tokenu može pristupiti i koristiti ga na isti način [5].

4. DECENTRALIZOVANE FINANSIJE

Decentralizovane finansije (eng. *Decentralized Finance* - *DeFi*) predstavljaju oblast u razvoju koja obuhvata presek blockchain-a, digitalne imovine (eng. *digital assets*) i finansijskih servisa. *DeFi* je opšti termin za decentralizovane aplikacije (*DApp*) koje pružaju finansijske usluge na blockchain-u, uključujući plaćanja, pozajmice, trgovanje, ulaganje i upravljanje imovinom. *DeFi* servisi tipično rade bez centralizovanog posrednika ili institucije i koriste otvorene protokole koji dozvoljavaju servisima da budu programski iskombinovani na fleksibilne načine [12].

4.1. Problemi koje *DeFi* rešava

DeFi nudi potencijal za rešavanje pet ključnih problema koji su povezani sa tradicionalnim centralizovanim finansijama [13]:

1. **Neefikasnost** - *DeFi* može da izvrši finansijske transakcije sa velikom količinom imovine i malim transakcionim troškovima, što bi generalno bio veliki organizacioni teret za tradicionalne finansije.
2. **Ograničeni pristup** - *DeFi* omogućava svim korisnicima pristup celoj finansijskoj infrastrukturi bez obzira na njihovo bogatstvo i geografsku lokaciju.
3. **Nedostatak transparentnosti** - *DeFi* elegantno rešava ovaj problem kroz otvorenu prirodu dogovora. Pametni ugovori direktno obezbeđuju transparentnost. *DeFi* smanjuje rizik da druga strana neće ispoštovati dogovor.
4. **Centralizovana kontrola** - *DeFi* ovo sprečava tako što prepušta kontrolu otvorenim protokolima koji imaju transparentne i neizmenljive karakteristike.
5. **Nedostatak interoperabilnosti** - Razlog za veliki rast *DeFi* ekosistema je mogućnost lakog kombinovanja *DeFi* proizvoda. Tokenizacija je ključan način na koji se *DeFi* platforme međusobno integrišu.

4.2. Decentralizovane platforme za pozajmljivanje

Pozajmice/krediti su esencijalan deo *DeFi* ekosistema. Postoji veliki broj različitih protokola koji omogućavaju ljudima da daju i uzimaju pozajmice (eng. *lending & borrowing*) u vidu kripto imovine. Decentralizovane platforme za kredite su jedinstvene po tome što ne zahtevaju od zajmodavaca (eng. *lenders*) i zajmoprimaca (eng. *borrowers*) da otkriju svoj identitet. Svi imaju pristup platformi i potencijalno mogu da pozajme novac ili da obezbeđuju likvidnost kako bi zaradili profit. Kao takve, *DeFi* pozajmice su potpuno bez ograničenja (eng. *permissionless*) i ne zasnivaju se na potrebi za poverenjem [14].

Postoje trenutne pozajmice (eng. *flash loans*) gde zajmoprimac dobije sredstva, koristi ih i isplati sve u sklopu jedne blockchain transakcije. One omogućuju korisnicima da pozajmljuju bez potrebe za zalogom. Takođe, postoje i pozajmice koje su pokrivene zalogom (eng. *collateralized loans*), gde je zalog zaključan u pametnom ugovoru i vraća se kada je dug isplaćen [12, 14].

5. IMPLEMENTACIJA

U ovom poglavlju je objašnjena implementacija decentralizovane finansijske aplikacije za štednju i uzimanje pozajmica na Ethereum platformi.

Implementirana aplikacije je nazvana Decentralizovana banka (eng. *Decentralized Bank*) i pruža mogućnost zajmodavcima da ulože ETH u banku, što predstavlja pozajmljivanje (eng. *lending*), a istovremeno i vid štednje, jer za to dobijaju nagrade u vidu novokreiranih ERC20 tokena aplikacije koji se zove *Decentralized Bank Token* (DBT). Takođe, pruža mogućnost zajmoprimcima da pozajme određenu količinu DBT tokena sa kamatom, a kao zalog moraju da ostave određenu količinu ETH.

Kako je Ethereum javni otvoreni blockchain bez permisija (eng. *permissionless*), tako ne postoji ograničenje kada su u pitanju korisnici koji mogu da koriste ovu aplikaciju. Svako može da koristi aplikaciju ukoliko ima instaliran MetaMask novčanik, koji predstavlja ekstenziju pretraživača, i ukoliko u njemu ima dovoljno ETH.

Svakom korisniku koji se sa svojim novčanikom poveže na aplikaciju su dostupne četiri funkcionalnosti koje pod određenim uslovima može da koristi. U te funkcionalnosti spadaju: ostavljanje depozita prilikom čega korisnik stavlja svoja sredstva na štednju (eng. *deposit*), povlačenje sredstava koja su prethodno ostavljena na štednju (eng. *withdraw*), uzimanje pozajmica (eng. *borrow*) i isplaćivanje pozajmica (eng. *pay off*).

Arhitektura sistema Decentralizovane banke je poprilično jednostavna i ona obuhvata bekend deo kojeg čine pametni ugovori koji su isporučeni (eng. *deploy*) na Ethereum blockchain, odnosno na Rinkeby test mrežu, i frontend deo kojeg čini React aplikacije koja je *deploy*-ovana na IPFS (InterPlanetary File System), koji predstavlja decentralizovan sistem za skladištenje sa adresabilnim sadržajem koji distribuira skladištenje objekata po čvorovima u *peer-to-peer* mreži.

Prvo sa čim se korisnik Decentralizovane banke susreće je web pretraživač pomoću koga dobija pristup frontend aplikaciji *deploy*-ovanoj na IPFS. Pretraživač isporučuje sadržaj aplikacije sa IPFS-a nakon što se pristupi specifičnom URL-u (eng. *Uniform Resource Locator*) koji će sadržati heš *deploy*-ovanih resursa. Kada se učita frontend aplikacija u pretraživač, korisnik ostvaruje interakciju sa Ethereum blockchain-on pomoću web3.js biblioteke kroz MetaMask novčanik.

Bekend deo čine dva pametna ugovora, koji su pisani u Solidity programskom jeziku. Za razvoj i testiranje pametnih ugovora korišćeni su Truffle radni okvir, Ganache lokalni blockchain i biblioteke za testiranje pametnih ugovora – Chai i Mocha.

Prvi pametni ugovor predstavlja ERC20 token koji je nazvan *Decentralized Bank Token* (DBT). DBT predstavlja token aplikacije Decentralizovane banke koja ga izdaje u vidu nagrada i pozajmica korisnicima sistema prilikom korišćenja njenih usluga. Ovaj pametni ugovor implementira ERC20 standard, kojeg čini određeni skup obaveznih funkcija i događaja koji svaki token mora da implementira. Takođe, ugovor sadrži i dodatne funkcije koje su potrebne za funkcionisanje Decentralizovane banke.

Drugi pametni ugovor je ugovor Decentralizovane banke koji predstavlja glavni ugovor aplikacije koji obavlja svu poslovnu logiku. Ovaj ugovor omogućava pozajmljivanje (eng. *Lending & Borrowing*) i ima četiri funkcije: *deposit*, *withdraw*, *borrow* i *payOff*. Takođe, ima i nekoliko promenljivih stanja koje skladište relevantne podatke o korisnicima sistema.

Funkcija *deposit* omogućava korisnicima da ostave depozit u ETH za štednju (eng. *lending*). Funkcija *withdraw* omogućava korisnicima da podignu svoj ETH koji su stavili na štednju i da za to dobiju nagradu u vidu DBT tokena, koja zavisi od veličine depozita i od vremena koje je proteklo od početka štednje, a gde je godišnji procentualni prinos 10% (Slika 2). Funkcija *borrow* omogućava korisnicima da pozajme DBT tokene pri čemu moraju da ostave zalog u ETH. Zalog mora da bude veći od pozajmljene količine tokena (eng. *overcollateralization*). Funkcija *payOff* omogućava korisnicima da vrate pozajmice pri čemu im se naplaćuje kamata od 10%, tako da nazad dobijaju 90% zaloga.

```
function withdraw() public {
    require(isDeposited[msg.sender] == true,
     'Error, no previous deposit');

    uint userBalance = etherBalanceOf[msg.sender];
    uint depositTime = block.timestamp - depositStart[msg.sender];
    uint interestPerSecond = 31668017 *
    (etherBalanceOf[msg.sender] / 1e16);
    uint interest = interestPerSecond * depositTime;

    msg.sender.transfer(userBalance);
    dbToken.mint(msg.sender, interest);
    earnedTokens[msg.sender] += interest;

    depositStart[msg.sender] = 0;
    etherBalanceOf[msg.sender] = 0;
    isDeposited[msg.sender] = false;

    emit Withdraw(msg.sender, userBalance,
     depositTime, interest, block.timestamp);

}
```

Slika 2. *Withdraw funkcija*

6. ZAKLJUČAK

U ovom radu je opisana implementacija koncepta decentralizovanih finansija u vidu aplikacije za štednju i uzimanje pozajmica, korišćenjem Ethereum platforme kao osnove za razvoj rešenja. Objašnjena je blockchain tehnologija sa fokusom na Ethereum. Objašnjen je pojam decentralizovanih finansija i koje probleme rešavaju. Opisani su korišćeni alati i tehnologije za razvoj, kao i arhitektura sistema i implementacija.

Implementacija ovog rešenja predstavlja uprošćenu verziju jedne realne *DeFi* aplikacije koja ima ulogu decentralizovane banke i obezbeđuje osnovne usluge štednje i uzimanja pozajmica. Jedno od poboljšanja aplikacije bi moglo biti pružanje mogućnosti štednje i ostavljanja zaloga korišćenjem različitih kriptovaluta, a ne samo ETH i DBT tokena.

7. LITERATURA

[1] Distributed Ledger Technology Systems - A Conceptual Framework, M. Rauchs, A. Glidden, B. Gordon, G. Pieters, M. Recanatini, F. Rostand, K. Vagneur, B. Zhang, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf

[2] Mastering Blockchain, I. Bashir

[3] Distributed Ledger Technology and Blockchain, World Bank Group, https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

[4] Global Blockchain Benchmarking Study, Dr G.Hileman, M. Rauchs, https://cdn.crowdfundinsider.com/wp-content/uploads/2017/09/2017-Global-Blockchain-Benchmarking-Study_Hileman.pdf

[5] Mastering Ethereum, A. M. Antonopoulos

[6] Ethereum Whitepaper, https://ethereum.org/en/whitepaper/

[7] Blockchain-Based Smart Contracts: A Systematic Mapping Study, M. Alharby, A. Moorsel, https://arxiv.org/ftp/arxiv/papers/1710/1710.06372.pdf

[8] Ethereum EVM illustrated, T. Takenobu, https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf

[9] Ethereum Yellow Paper, https://ethereum.github.io/yellowpaper/paper.pdf

[10] Proof-of-Work, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/

[11] Proof-of-Stake, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[12] DeFi Beyond the Hype, https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

[13] Defi and the Future of Finance, https://www.prophecydefi.com/_resources/media/Harvard_DeFi_and_the_Future_of_Finance.pdf

[14] Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

Kratka biografija:

Marina Bartulov je rođena u Novom Sadu 1997. god. Osnovne akademske studije završila je 2020. godine na Fakultetu tehničkih nauka u Novom Sadu. Master rad na Fakultetu tehničkih nauka iz oblasti Računarstvo i automatika – Elektronsko poslovanje odbranila je 2022. godine.