Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 007:004.056
DOI: https://doi.org/10.24867/18BE22Grujic

POZAJMLJIVANJE U KRIPTO VALUTAMA

CRYPTOCURRENCY LENDING

Aleksandra Grujić, *Fakultet Tehničkih Nauka, Novi Sad*

Oblast – RAČUNARSTVO I AUTOMATIKA

Kratak sadržaj – *U ovom radu opisana je arhitektura sistema za pozajmljivanje u kripto valutama i način na koji funkcioniše pomoću pametnih ugovora. Pored toga opisani su centralizovani i decentralizovani sistemi i njihove prednosti i mane, kao i osnovni koncepti distribuiranih sistema i blokčejn tehnologije sa fokusom na Ethereum-u.*

Ključne reči: *distribuirani sistemi, blokčejn, pametni ugovori, pozajmljivanje u kripto valutama*

Abstract – *In this work we described crypto lending and the way in which it works via smart contracts. Besides that, we describe centralized and decentralized systems and its advantages and disadvantages, as well as the fundamentals of distributed systems and blockchain technology with focus on Ethereum.*

Keywords: *distributed systems, blockchain, smart contract, crypto lending*

1. UVOD

Tema ovo rada jeste kripto pozajmljivanje koje je danas sve popularnije među ljudima, a koje omogućava da ljudi pozajmljuju novac tj. uzimaju ukoliko im je potreban, ali i da oni svoj novac pozajmljuju tj. daju i na taj način zarade. Kripto pozajmljivanje je moguće primenjivati u centralizovanim i decentralizovan sistemima tako da će u nastavku biti objašnjena razlika između njih i koje su prednosti i mane. Nakon toga će biti opisani distribuirani sistemi, blokčejn tehnologija, Ethereum i njegov blokčejn, kao i šta su i čemu služe pametni ugovori. Nakon teorijskih osnova biće opisano pozajmljivanje u kripto-valutama, ko su učesnici i koraci samog procesa. Osim teorijskog dela o kripto pozajmljivanju, opisana je i aplikacija koja predstavlja način na koji ono funkcioniše.

2. BLOKČEJN

2.1. Centralizovani i decentralizovani sistemi

Iako svi sistemi mogu da funkcionišu efikasno, neki su stabilniji, a neki sigurniji. Neki sistemi su jako mali i povezuju nekoliko uređaja i mali broj korisnika, dok su neki ogromni i obuhvataju države i kontinente. U svakom slučaju, svi oni se suočavaju sa istim problemima kao što su tolerancija na greške, troškovi održavanja, skalabilnost i vreme potrebno za razvoj. Kada govorimo o centralizovanim i decentralizovanim sistemima govorimo o tome ko ima kontrolu nad celim sistemom.

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

Centralizovani sistemi su sistemi kod kojih postoji jedan centralni organ koji odlučuje o svemu i koji ima kontrolu nad svim podacima i funkcionalnostima u sistemu. Taj centralni organ može biti pojedinac ili grupa ljudi. Centralni organ čuva podatke kojima korisnici mogu pristupati, ali čuva i podatke o korisnicima kao sto su ime, prezime, datum rođenja itd. On ima prava da te podatke menja i briše bez bilo kakve dozvole.

Prednost ovih sistema je jednostavnost u donošenju odluka jer konačnu odluku uvek donosi jedna osoba. Oni su laki za održavanje i praktični su u slučaju kada je potrebno kontrolisati podatke centralno.

Međutim, centralizovani sistemi imaju veliko ograničenje, a to je da ukoliko centralni organ prestane sa radom, ceo sistem više neće moći da funkcioniše i korisnici neće moći da pristupaju podacima. Pored toga, mana centralizovanih sistema je i ta da postoji zabrinutost korisnika za sigurnost i bezbednost podataka jer samo jedan vlasnik ima kontrolu nad svim podacima. To je razlog sto centralizovani sistemi nisu više prvi izbor većini organizacija [1, 2].

Decentralizovani sistemi nemaju jedan centralni organ tj. centralni autoritet koji ima kontrolu nad svim i donosi konačnu odluku, kao što je to slučaj kod centralizovanih sistema. Oni imaju više centralnih organa i svaki od njih čuva kopiju podataka kojima korisnici pristupaju.

Oni mogu biti podložni otkazima kao i centralizovani, ali su ipak više tolerantni na kvarove u sistemu. To je zbog toga što ukoliko jedan ili više centralnih organa padne, drugi će nastaviti da rade i omogućavati korisnicima pristup podataka. To je jedna od glavnih prednosti ovih sistema jer će podaci biti dostupni čak i ako samo jedan centralni organ nastavi sa radom.

Mana ovih sistema je bezbednost i privatnost podataka kao i kod centralizovanih sistema, a druga mana je to što je održavanje decentralizovanih sistema obično skuplje [1, 2].

2.2. Distribuirani sistemi

Distribuiran sistem je kolekcija nezavisnih računarskih elemenata koji svojim korisnicima izgleda kao jedinstven koherentni sistem. Ova definicija se odnosi na dve karakteristike distribuiranih sistema. Jedna se odnosi na to da je distribuiran sistem kolekcija računarski komponenti gde se svaka od njih ponaša nezavisno jedna od druge. Računarski element, koji ćemo zvati čvorom (engl. node - čvor), može biti ili hardverski uređaj ili softverski proces. Druga karakteristika je da korisnici, a to su ljudi ili aplikacije, veruju da rade sa jedinstvenom sistemom. To znači da autonomni čvorovi moraju međusobno da

sarađuju. Ukoliko čvorovi ignorišu jedni druge onda nema svrhe da se stavljaju u isti distribuirani sistem. Za postizanje zajedničkog cilja, potrebno je da međusobno interaguju razmenom poruka. Čvor prima poruku, obrađuje je i prosleđuje dalje [3, 4].

Nezavisnost čvorova jedni od drugih dovodi do toga da će svaki od njih imati svoj lokalni sat. To je razlog zbog kog ne postoji globalni sat (engl. global clock- globalni sat). Ovaj problem nepostojanja zajedničkog vremena dovodi do problema koji se tiču sinhronizacije između čvorova. Komunikacija se zasniva samo na slanju poruka putem mreže.

Sledeća bitna karakteristika distribuiranih sistema je konkurentnost. U ovom sistemu dozvoljeno je da više klijenata istovremeno pristupi istom resursu što znači da komponente sistema rade istovremeno.

Ono što je jako bitno za normalan rad sistema je da postoji nezavisan otkaz komponenti, to znači da otkaz pojedinačnih komponenti neće uticati na rad celog sistema.

Skalabilnost je sposobnost rasta sistema sa povećanjem obima posla i to je bitna karakteristika distribuiranih sistema. Ona se postiže dodavanjem dodatnih procesorskih jedinica ili čvorova u mrežu po potrebi [4].

2.3. Blokčejn tehnologija

Distribuirana baza podataka je vrsta baze podataka kod koje se podaci čuvaju u više čvorova. Distribuirana glavna knjiga ili tehnologija distribuirane glavne knjige je vrsta distribuirane baze podataka.

Blokčejn je distribuirana glavna knjiga (engl. distributed ledger- distribuirana glavna knjiga) koja se sastoji od svih transakcija koje su napravljene u blokčejnu. Transakcije su grupisane u blokove koji zajedno čine lanac blokova. U opštem slučaju, svaki učesnik će kod sebe imati identičnu kopiju lanca sa svim transakcijama [4].

Glavne karakteristike blokčejna su da je distribuiran, nepromenjiv i dogovaranje sa konsenzusom. Jedna od glavnih karakteristika blokčejna je da je on distribuirana glavna knjiga, što znači da je to baza podataka čiju kopiju imaju svi čvorovi kod sebe. Nema centralnog autoriteta koji ima i menja glavnu knjigu. Da bi se dodao novi blok u lanac potrebno je da se proveri da li je validan, a to se postiže pomoću konsenzus mehanizma. Jednom kada je novi blok odobren, svaki čvor ažurira svoju glavnu knjigu. Nasuprot tome, tradicionalne baze podataka su skladištene i održavaju se centralno, što ih može učiniti lakom metom za hakere i kriminalce.

Druga karakteristika je nepromenljivost. U suštini, jednom kada je transakcija dodata u blokčejn glavnu knjigu, ona ne može biti uklonjena. Nepromenljivost blokčejna osigurana je upotrebom kriptografije. Svaka transakcija sadrži neke informacije koje se heširaju pomoću kriptografskog heš algoritma. Za iste informacije će se uvek dobijati isti heš. Ukoliko se bilo koji podatak u bloku promeni, njegov heš će se promeniti i to će dovesti do promene sadržaja svih blokova koji idu posle njega jer svaki blok sadrži heš od prethodnog. Čvorovi će primetiti da su se podaci u celom lancu promenili i odbaciće tu verziju glavne knjige. Na ovaj način se obezbeđuje nepromenljivost blokčejn glavne knjige i čini je sigurnom.

Treća važna karakteristika blokčejna jeste dogovaranje sa konsenzusom. Nijedan blok ne može biti dodat u glavnu knjigu bez da to odobre čvorovi u mreži. To se postiže pomoću konsenzus mehanizma. Konsenzusi su ključni kada hoće da se osigura da je svaki blok u lancu validan i da se svi učesnici slažu da može da se doda u glavnu knjigu. Na taj način konsenzus algoritmi postižu pouzdanost blokčejn mreže i čine da čvorovi veruju mreži iako možda ne veruju jedan drugom [5, 6].

Blokčejn koristi konsenzus mehanizme od kojih su najpoznatiji Proof of work i Proof of stake … Čvorovi koji dodaju nove blokove u lanac se zovu engl. Miners. Oni se takmiče sa drugim minerima za dodavanje novog bloka u glavnu knjigu. Ako uspeju, dobijaju nagradu u vidu kriptovalute.

Proof-of-Work (PoW) je algoritam u kom miner treba da pronađe odgovarajući Nonce broj da bi dodao blok u lanac. To se postiže isprobavanjem različitih vrednosti Nonce broja da se dobije željeni rezultat. Zbog toga je bitno imati jak hardver, jer se više pokušaja može napraviti za kraće vreme i time se povećava šansa za dodavanje validnog bloka u lanac.

Najpopularniji alternativni algoritam za rudarenje je Proof-of-Stake (PoS). Kod ovog algoritma, rudari dobijaju nagradu koja nije srazmerna snazi njihovog hardvera već količini kriptovalute koju već poseduju.

2.4. Ethereum

Ethereum blokčejn je decentralizovana, distribuirana javna glavna knjiga u kojoj se sve transakcije verifikuju pa zatim upisuju. Distribuirana jer svi koji učestvuju u Ethereum mreži imaju kod sebe identičnu kopiju ove knjige i imaju mogućnost da vide sve transakcije koje u zapisane u njoj. Decentralizovana zbog toga što ne postoji centralni autoritet koji upravlja mrežom već njome upravljaju i menjaju je svi koji imaju kod sebe distribuiranu knjigu.

Ethereum platforma ima svoju kriptovalutu koja se zove Ether (ETH) ili Ethereum, i ima svoj programski jezik koji se zove Solidity. Ether je pre svega bio namenjen za korišćenje unutar Ethereum mreže, ali sada je prihvaćen kao oblik plaćanja od strane nekih trgovaca za određene usluge.

Ethereum želi da bude platforma za sve vrste aplikacija koje mogu da sigurno čuvaju informacije. On omogućava programerima da naprave i objavljuju smart contract-e, kao i da kreiraju igrice i aplikacije koje se zovu dApps. One se mogu koristiti bez rizika od pada sistema ili prevara. Korisnici plaćaju fees (engl. fee – naknada) za korišćenje dApps na Ethereum platformi. Ove naknade se nazivaju „gas“ jer variraju u zavisnosti od količine upotrebljene računarske snage [7].

Ethereum je trenutno proof-of-work (PoW) blokčejn ali je u planu da pređe na proof-of-stake (PoS) radi skalabilnosti i pristupa koji je ekološki prihvatljiviji.

2.5. Smart contract

Smart contract (engl. smart contract – pametan ugovor) je program koji se pokreće na na Ethereum mreži, odnosno kolekcija koda (njegove funkcije) i podataka (njegovo stanje), i nalazi se na određenoj adresi na Ethereum blokčejnu. To se zove ugovor jer taj kod koji se pokreće

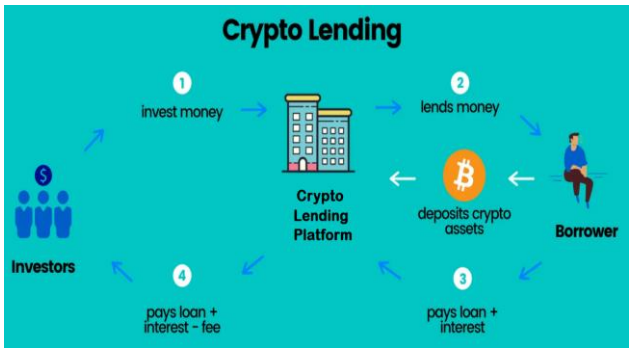
na Ethereumu može kontrolisati vredne stvari poput ETH-a ili druge digitalne imovine [8].

Jednom kada se smart contract nađe na Ethereum mreži, njegova definicija ne može da se menja. Ukoliko neko želi da izmeni postojeći smart contract koji je već na mreži, mora da doda novu verziju na novu adresu. Iz tog razloga, mora se obratiti pažnja na kvalitet koda i na testiranje da se ne bi unele neke greške koje nikad neće moći da se isprave.

Solidity je proceduralni programski jezik sa sintaksom koja je slična Java Script, C++ i Java programskim jezicima. To je najpopularniji i najčešće korišćen jezik za pisanje Ethereum pametnih ugovora.
Ethereum virtualna mašina (EVM) se nalazi na svakom čvoru na mreži i radi kao lokalna instanca, ali pošto sve instance EVM-a rade na istom početnom stanju i proizvode isto konačno stanje, sistem u celini funkcioniše kao jedan „svetski računar“. Na EVM-u se pokreće specijalna forma koda koja je zove EVM bajtkod. Iako je pametne ugovore moguće pisati direktno u bajtkodu, EVM bajtkod je programerima prilično težak za razumevanje. Umesto toga, većina programera koristi jezike visokog nivoa za pisanje programa i kompajler za pretvaranje u bajt kod [9].

3. POZAJMLJIVANJE U KRIPTOVALUTAMA

Tradicionalni finansijski servisi, kao sto je dobijanje kredita, bilo je jedino dostupno preko zvaničnih finansijskih institucija i banaka. To se promenilo uvođenjem blokčejn tehnologije. Dobijanje kredita sa kriptovalutama je često manje komplikovan proces nego dobijanje tradicionalnih bankovnih kredita. Pored dobijanja kredita odnosno zaduživanja, zahvaljujući blokčejnu uvedeno je i pozajmljivanje kriptovaluta i mogućnost zarade na taj način [10].



Slika 1. *Proces pozajmljivanja u kriptovalutama*

3.1. Zaduživanje u kriptovalutama

Zaduživanje u kriptovalutama podrazumeva dizanje kredita koje je slično tradicionalnom dizanju kredita gde se koristi imovina, u ovom slučaju kriptovalute kao zalog za kredit [11].

Neke od karakteristika kripto kredita su:

1. Kamatne stope su relativno niske
2. Ograničeno je koliko može da se pozajmi - većina platformi dozvoljava da se pozajmi 50% od vrednosti nečije kriptovalute. Sredstva kredita mogu da se dobiju u obliku američkih dolara ili druge izabrane digitalne valute
3. Nema provere kreditne sposobnosti – što znači da je dizanje kredita pristupačnije ljudima koji imaju promenljiva primanja pa ne ispunjavaju bankovne uslove za kredit
4. Dobijanje kredita traje svega par sati – dok dobijanje bankovnih kredita može potrajati i po nekoliko dana, kripto krediti se dobijaju gotovo odmah

3.2. Pozajmljivanje u kriptovalutama

Sa druge strane, pozajmljivanje u kriptovalutama omogućava onima koji imaju kriptovalute da zarade kamatu na svojoj imovini kada je pozajmljuju nekome. Funkcioniše tako što onaj ko pozajmljuje plaća kamatu u zamenu za korišćenje nečije imovine, odnosno kriptovaluta. Najbolje kamatne stope su obično rezervisane za stablecoin-e, digitalna imovina koja ne menja puno vrednost, kao što su FIAT valute poput američkog dolara ili za zlato [12].

4. IMPLEMENTACIJA APLIKACIJE ZA KRIPTO POZAJMLJIVANJE

Aplikacija koja će se opisivati je aplikacija koja se koristi za crypto lending. Ona predstavlja proces na koji funkcioniše pozajmljivanje, odnosno dizanje kredita bazirano na kriptovalutama. U daljem tekstu će biti reči o alatima i tehnologijama koje su se koristile za njenu realizaciju, kao i opis samih funkcionalnosti.

Učesnici u samom procesu su *lender* (engl. lender –zajmodavac) koji pozajmljuje novac nekome i *borrower* (engl. borrower – zajmoprimac) koji taj novac uzima odnosno diže kredit. Oni imaju svoje naloge na MetaMask-u, gde svako od njih ima svoju adresu i imovinu u obliku kriptovalute. MetaMask je ekstenzija za pretraživač koja omogućava i olakšava komunikaciju sa Ethereum blokčejnom. Drugim rečima, MetaMask je novčanik koji je stvoren za rad Ethereum blokčejnom i osmišljen je kako bi korisnicima omogućio da u potpunosti kontrolišu svoje podatke i imovinu, kao i da se transakcije izvršavaju brzo i lako.

Uslovi kredita kao i funkcije koje omogućavaju prenos sredstava sa jedne adrese na drugu se nalaze u *smart contract*-u. *Smart contract* je pisan u jeziku Solidity u Remix-u i ima .sol ekstenziju. Remix je *online* razvojno okruženje koje se koristi za olakšano kreiranje i deployovanje tj. objavljivanje *smart contract*-a na mrežu.

Pre svega potrebno je napraviti ERC20 token. ERC20 je standard koji se koristi za *smart contract*-e na Ethereum blokčejnu za implementaciju tokena i obezbeđuje listu pravila koje svi Ethereum tokeni moraju da zadovoljavaju.

Proces započinje *lender* koji deo svoje imovine u ERC20 tokenima šalje na *smart contract*. Pre toga je potrebno dozvoliti *smart contract*-u da može da skine sredstva sa računa *lendera*, kao i koji iznos može da skine. Nakon toga *borrower* uzima ta sredstva sa *smart contract*-a i na taj način diže kredit, ali da bi to uradio mora da određeni deo svoje ETH imovine priloži kao *collateral* (engl. collateral – zalog) koji je veći od iznosa koji uzima za kredit. Na kraju, *borrower* vraća kredit tako što vraća iznos koji je podigao, ali i kamatu. *Lender* na ovaj način može da zaradi kamatu koju *borrower* mora da plati jer je digao kredit. Ukoliko *borrower* ne ispoštuje dogovor i ne otplati kredit do datuma do kog je dogovoreno, *lender*

ima pravo da uzme ceo iznos koji je *borrower* priložio kao zalog. Na taj način je *lender* osiguran i ne postoji mogućnost da ne dobije nazad novac koji je pozajmio.

```
function fundLoan() public{

    DAI(daiAddress).transferFrom(
        msg.sender,
        address(this),
        terms.loanDaiAmount
    );
}

function takeALoanAndAcceptLoanTerms() public payable{

    require(msg.value == terms.ethCollateralAmount,
            "Invalid collateral amount");

    borrower = payable (msg.sender);
    DAI(daiAddress).transfer(
        borrower,
        terms.loanDaiAmount);
}

function repay() public{

    require(msg.sender == borrower,
            "Only the borrower can repay the loan");

    DAI(daiAddress).transferFrom(
        borrower,
        lender,
        terms.loanDaiAmount + terms.feeDaiAmount);

    selfdestruct(borrower);
}
```

Slika 2. Smart contract

Za testiranje aplikacije je korišćena testna mreža na Ethereum platformi koja se zove Ropsten Test Network. To je mreža koja je kopija prave Ethereum mreže koja omogućava svakome da proba mrežu bez potrebe za pravim ETH novčićima. Da bi se dobili novčići na mreži korišćen je Ropsten Ethereum Faucet. Prilikom slanja zahteva za dobijanje novčića potrebno je uneti adresu naloga na koju će stići novčići. Po jednom zahtevu može se dobiti pet novčića, a za narednih pet se mora čekati da prođe dvadeset četiri sata. Dakle, to su testni novčići koji nemaju pravu vrednost i koriste se samo u svrhu testiranja pametnih ugovora, kao i za transakcije jer se svaka izvršena transakcija na mreži naplaćuje.

5. ZAKLJUČAK

U ovom radu opisana je blokčejn tehnologija, način na koji funkcioniše kao i njene glavne karakteristike. S obzirom na to da se bazira na nepromenljivosti informacija, čini je pogodnom i za mnoge druge sfere pored finansijske.

Fokus ovog rada je na kripto pozajmljivanju, što predstavlja samo jednu od mnogih funkcionalnost koje se mogu izvršavati na blokčejnu. Kripto pozajmljivanje postaje sve popularnije s obzirom na to da je postupak dobijanja kredita mnogo jednostavniji u odnosu na tradicionalno dizanje kredita. Pored toga, za razliku od tradicionalnih kredita, ljudi neće biti podložni proceni njihove kreditne sposobnosti što znači da je pristupačniji ljudima koji nemaju stalna primanja ili koji nisu zaposleni.

Postupak kripto pozajmljivanja implementiran je u aplikaciji uz pomoć pametnih ugovora. U pametnom ugovoru definisani su uslovi ugovora između onog ko daje pozajmicu i ko je prima. Zahvaljujući tome oni ne moraju da veruju jedan drugome ali pametni ugovor neće dozvoliti da se navedeni uslovi prekrše.

6. LITERATURA

[1] Centralized vs Decentralized vs Distributed systems https://berty.tech/blog/decentralized-distributed-centralized

[2] Difference between Centralized, Decentralized and Distributed systems https://www.scaleyourapp.com/difference-between-centralized-decentralized-distributed-systems-explained/

[3] Distributed Systems, Third edition, Maarten van Steen, Andrew S. Tanenbaum

[4] Paralelni i distribuirani algoritmi i strukture podatakaDr Dušan Gajić, FTN izdavastvo, 2019, http://www.acs.uns.ac.rs/sr/filebrowser/download/5150364

[5] 6 key Blockchain features https://101blockchains.com/introduction-to-blockchain-features/

[6] OECD Blockchain Primer https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

[7] What is Ethereum and how does it work ? https://www.forbes.com/advisor/investing/what-is-ethereum-ether/

[8] Introduction to smart contracts https://ethereum.org/en/developers/docs/smart-contracts/

[9] Mastering Ethereum Andreas M. Antonopoulos, Gavin Wood https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc

[10] Crypto Lending: What is it ? https://crowdfunding-platforms.com/crypto-lending

[11] What is crypto lending and how does it work ? https://www.bankrate.com/loans/personal-loans/cryptocurrency-lending/

[12] What is crypto lending ? https://loans.usnews.com/articles/what-is-crypto-lending

Kratka biografija:

Aleksandra Grujić rođena je u Novom Sadu 1995. god. Osnovne akademske studije završila je 2018. godine na Fakultetu tehničkih nauka u Novom Sadu. Master rad na Fakultetu tehničkih nauka iz oblasti Računarstvo i automatika – Elektronsko poslovanje odbranila je 2021. godine.