Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/14BE07Jocovic

POSLOVNI PROCESI U KOLABORACIJI SA BLOKČEJNOM

BUSINESS PROCESSES IN COLLABORATION WITH BLOCKCHAIN

Zorka Jocović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – Primenjene računarske nauke (Elektronsko poslovanje)

Kratak sadržaj – *Ovaj rad predstavlja istraživanje mogućnosti integrisanja poslovnih procesa i blokčejna,. Poslovne procese karakteriše tačan redosled akcija da bi se izvršio neki posao, te su oni pogodni za upotrebu kod aplikacija koje imaju jasno definisan tok operacija. Kao primer u ovom radu korišćeno je rezervisanje automobila. Ovakva aplikacija je pogodna za korišćenje i Blokčejn tehnologije, jer zahteva nekoliko faza u kojima se mora postići konsenzus (garancija) da su ispunjeni svi uslovi oko kojih se dogovaraju klijent koji iznajmljuje auto i agent koji izdaje isti.*

Ključne reči: *bpmn, blokčejn, pametni ugovor, ethereum, transakcija, adresa, rudarenje*

Abstract – *This paper presents research of the possibilities of business processes, blockchain and their integration. Business processes are characterized by the exact sequence of actions to perform a job, so they are suitable in applications that have a clearly predefined flow. For example, in this paper is used Rent A Car application. The application is suitable for the use of Blockchain technology, as it requires several stages in which a consensus must be reached to meet all the conditions agreed between client and agent.*

Keywords: *bpmn, blockchain, smart contract, ethereum, transaction, address, mining*

1. UVOD

Odnedavno se tehnologija lanca blokova (eng. *blockchain* – u nastavku rada koristiće se izraz blokčejn) počela koristiti u različitim sektorima, kao što su industrija i istraživanje. Razlog povećanog interesa za ove tehnologije jeste taj što aplikacije bazirane na blokčejnu mogu da rade distribuirano, bez potrebe za nekim posrednikom, ili pomoću treće strane, koja bi pregovarala i garantovala interese svih strana.
Blokčejn omogućava čuvanje digitalnih podataka uz minimalne troškove i može sprovoditi sve ono što su se dve strane dogovorile i garantovati neopozivo stanje ugovora.

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

Blokčejn tehnologije, iako prvenstveno poznate kao osnovna platforma za kripto valute, nalaze svoje primene na različite načine, a jedan od sve bitnijih jeste primena „pametnih ugovora“ (eng. *smart contracts*). U ovom radu prikazana je implementacija pametnih ugovora koji se nalaze i izvršavaju na blokčejnu, a preko kojih se obezbeđuje interakcija poslovnih procesa zainteresovanih strana. Pametni ugovor predstavlja samoizvršivi bajt kod (eng. *byte code*) koji omogućava izvršavanje opisanih, dogovorenih stavki strankama.

2. BLOKČEJN TEHNOLOGIJA

Tokom 2008. godine na Internetu se pojavila publikacija anonimnog autora, pod pseudonimom Satoši Nakamoto, koji je predložio decentralizovani sistem elektronskog novca [1]. Ideja o elektronskom novcu nije bila novina u to vreme, ali je ovaj rad detaljno opisao moguću implementaciju koja bi bila distribuirana i kriptografski sigurna koristeći koncept dokaza utrošene računarske snage (eng. *Proof of Work*) pomoću kojeg se postizao konsenzus između učesnika sistema.
Blokčejn je baza podataka koja se ne nalazi na jednom mestu, već je čine manje baze (blokovi) koje su međusobno digitalno povezane, a koje sadrže informacije o digitalnim transakcijama bilo koje vrste: od vlasničkih listova, preko podataka iz knjige rođenih, do ugovora kojim se regulišu autorska prava. Prilikom njihove razmene nema nikakvog regulatora osim same mreže koja sadrži informacije o svim transakcijama koje su ikada izvedene. Svaka promena podataka u ovoj bazi se sprovodi po unapred definisanim pravilima i svaki učesnik sistema mora verifikovati istu. Dakle, za razliku od klasične *online* baze podataka, blokčejn omogućava komunikaciju sa nekoliko računara (servera) između kojih se obavlja transakcija.

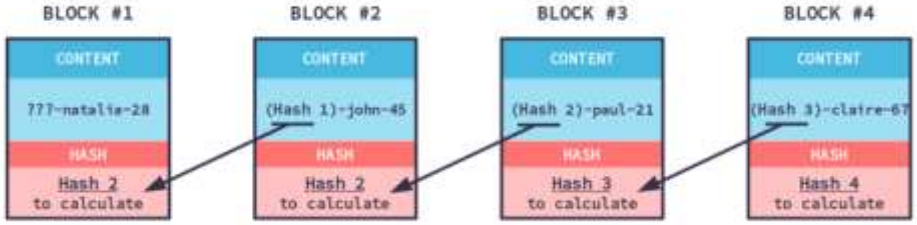
2.1. Adrese

Pripadnost određenih sredstava - bilans (eng. *balans*) na blokčejn platformi je vezana za adresu. Za formiranje adrese neophodno je generisati par ključeva (privatni i javni) ECDSA šemom. Korisnik može da podeli svoju adresu u svrhu primanja sredstava od drugih korisnika. Par privatnog i javnog ključa, kao i adresa koja je izvedena iz javnog ključa, često se zajedno nazivaju (elektronski) novčanik (eng. *wallet*).

2.2. Rudarenje

Rudarenje (eng. *mining*) je proces kreiranja novih blokova u svrhu održavanja cele mreže koje sa sobom nosi i

finansijski podsticaj (nagradu). Učesnici sistema koji imaju dovoljnu količinu kompjuterskih resursa za rudarenje mogu pristupiti ovom procesu i nadmetati se. Učesnik koji prvi izrudari blok biva nagrađen određenom količinom *Bitcoin*-a, *Ether*-a ili neke druge kriptovalute u zavisnosti od tipa blokčejna.
Rudarenje se svodi na heširanje zaglavlja bloka dok dobijena heš vrednost ne ispunjava određene uslove. Uslov je da heš vrednost bude manja od određene vrednosti koja je trenutna težina rudarenja koja se kalkuliše u sistemu. Svaka iteracija algoritma rudarenja se sprovodi sa drugom vrednošću polja *nonce*. I najmanja promena ulaznih podataka zaglavlja bloka rezultuje velikom promenom izlaza heš funkcije, što omogućava da se algoritam iznova pokušava, sve dok se uslov ne ispuni. Kada se ispuni uslov, blok se šalje svojim susedima i propagira po celoj mreži i kreće nadmetanje za sledeći blok. Na slici 1 prikazan je lanac blokova.



Slika 1. *Lanac blokova [2]*

2.3 Pametni ugovori

Pametni ugovori predstavljaju glavni koncept implementiran na *Ethereum* [3] blokčejn platformi. U osnovi, pametni ugovor je računarski program koji verifikuje i izvršava svoje uslove po nastanku unapred određenih događaja. Njih odlikuje svojstvo da se nakon smeštanja na blokčejn više ne mogu promeniti. Ovim mehanizmom se može obezbediti smanjenje rizika između učesnika koji nemaju uspostavljeno međusobno poverenje tako što mogu da prihvate ili da odbiju interakciju sa pametnim ugovorom nakon inspekcije njegove sadržine tj. programskog/bajt koda.
Dakle, pametni ugovori se ne sprovode u skladu sa zakonima određene zemlje, kao kod standardnih pisanih ugovora, gde se primenom tih zakona osiguravaju određeni uslovi, već funkcionišu tako što je sve ono što se mora ispuniti napisano u ugovoru. Ovakvim rešenjem se zaista eliminiše bilo koja vrsta posrednika.
Kada je u pitanju *Ethereum* blokčejn, koji u osnovi predstavlja distribuiranu bazu podataka, čvorovi mreže moraju biti u mogućnosti da postignu dogovor o trenutnom stanju sistema, što se postiže mehanizmom konsenzusa. Konsenzus mehanizmi ili protokoli omogućavaju pouzdanu komunikaciju između nepoverljivih strana. Trenutno se koriste PoW *(Proof of Work) i* PoS *(Proof of Stake)* mehanizmi.

3. POSLOVNI PROCESI

Upravljanje poslovim procesima (eng. *Business Process Management – BPM*) bavi se dizajnom, analizom, izvršenjem, praćenjem, automatizacijom i unapređenjem poslovnih procesa. Zasniva se na postavci da je svaki proizvod (usluga), koju određena kompanija (organizacija) nudi tržištu, rezultat obavljanja niza aktivnosti u kompaniji.

Poslovni proces se izvršava u okviru jedne organizacije. Sistem za upravljanje poslovnim procesima može se koristiti za uspostavljanje kontrole nad poslovnim procesom (orkestracija). Što se tiče korisnika ovakve vrste sistema, to su menadžeri (organizacioni nivo) i IT sektor (istraživači i programeri). Za modelovanje poslovnih procesa koristi se BPMN (eng. *Business Process Model Notation*).

Dakle, proces je niz operacija koje se izvode u uređenom redosledu koji je određen skupom poslovnih pravila. Proces se može definisati i kao strukturirani niz aktivnosti koje pokreće određeni događaj (ili više njih), a čiji je zadatak ostvarivanje (rezultat) određenog cilja (Slika 2). Proces koristi resurse prilikom ostvarivanja definisanog cilja, podložan je spoljašnjim uticajima i njime treba upravljati.

Slika 2. Definicija procesa

3.1. BPMN – Business Process Model Notation

BPMN (eng. *Business Process Model Notation*) se koristi za modelovanje poslovnih procesa. Primarni cilj BPMN-a bio je pružiti zapis koji je svima lako razumljiv u nekom sistemu poslovnih korisnika; od poslovnih analitičara koji kreiraju početne nacrte procesa, do programera koji su odgovorni za primenu tehnologije koja će implementirati procese i konačno, poslovnim ljudima koji će upravljati i nadgledati te procese (menadžeri).

BPMN stvara most između dizajna poslovnog procesa i implementacije procesa. On definiše dijagram poslovnog procesa, koji se zasniva na tehnici dijagrama toka i koristi grafički model poslovnog procesa.

Model poslovnog procesa je u suštini graf objekata, koji predstavljaju aktivnosti (tj. zadatak) i tok koji kontroliše redosled izvršavanja istih.

BPMN notacija definiše skup grafičkih elemenata koji se mogu koristititi za formiranje modela procesa. Ovi elementi omogućavaju lak razvoj jednostavnih dijagrama, koji će većini poslovnih analitičara izgledati poznato (npr. *flowchart diagram*). Elementi koji se koriste se međusobno razlikuju po obliku, ali su slični u većini alata

za modelovanje. Glavni cilj modela jeste stvaranje jednostavnog mehanizma za kreiranje modela poslovnih procesa, koji je istovremeno u stanju da se nosi sa složenošću poslovnog procesa. Pristup preduzet za ispunjavanje ova dva sukobljena zahteva jeste da se grafički aspekti notacije organizuju u određene kategorije.

3.2. Koreografije u BPMN-u

Koreografija predstavlja više poslovnih procesa u kome različite organizacije (poslovni partneri) obavljaju međusobnu interakciju. Da bi se pravilno izmodelovala, ne moraju se poznavati svi koraci koje organizacije obavljaju, ali je neophodno znati u kojim tačkama internih procesa je neophodno ostvariti interakciju između procesa. Koreografski jezici pružaju sredstvo za preciziranje razmenjenih poruka između organizacija, zajedno sa ograničenjima u ponašanju [2]. BPMN sadrži veliki skup grafičkih elemenata za modelovanje ovakvih procesa, zbog čega se i koristi u ovom radu.

Koncepti koreografije su vrlo značajni za ovaj rad, jer predstavljaju osnovno sredstvo komunikacije između organizacija koje su korišćene u primeru aplikacije

4. OPIS FUNKCIONALNOSTI APLIKACIJE ZA IZNAJMLJIVANJE AUTOMOBILA

Kao što je već spomenuto, aplikacija koja će se analizirati u ovom radu jeste *web* aplikacija koja se koristi za iznajmljivanje automobila od *Rent A Car* kompanije, oslanjajući se na već analizirane tehnologije (blokčejn i *BPM*).

Ugovorne strane koje će učestvovati u ovom sistemu su diler, odnosno agent koji se bavi iznajmljivanjem automobila, dok je sa druge strane klijent kao korisnik automobila. Ulogu posrednika obavljaće blokčejn komponenta, koja će automatski "zapisivati" sve stavke ugovora oko kojih se dogovore stranke.

Sam proces počinje poručivanjem automobila od strane klijenta, odnosno slanjem upita za željenim automobilom. Agentu pristiže porudžbina od klijenta, on je analizira i odlučuje da li može da ispuni zahteve. Ukoliko može i ima traženi automobil na stanju, šalje ponudu klijentu sa uslovima najma. Potom klijent pregleda ponudu pristiglu od agenta i odlučuje da li mu ponuđeni uslovi odgovaraju ili ne. Ukoliko mu ne odgovaraju, on je odbija i sam proces se terminira. Međutim, ukoliko prihvati ponudu, ugovor se dodaje u blokčejn i agent dobija obaveštenje da je klijent prihvatio ponudu, a agent obaveštava kupca da je auto spreman za preuzimanje. U pametni ugovor se upisuju sve stavke iz ponude agenta na koje je kupac pristao. U ponudi agenta, uneo je cenu depozita koju klijent mora platiti pre nego preuzme auto. Informacija da je klijent platio depozit se takođe beleži u ugovoru. Kada klijent završi sa vožnjom iznajmljenog automobila, on ga vraća nazad agentu. Agent proverava da li je automobil oštećen dok je bio kod klijenta. Ako nema oštećenja, klijent plaća najam umanjen za visinu depozita koji je plaćen prilikom preuzimanja aautomobila. Ukoliko pak postoje određena oštećenja, agent procenjuje vrednost štete i dostavlja račun klijentu. Potom klijent plaća cenu sa računa, u zavisnosti od potencijalnih oštećenja i tu se završava tok aplikacije. Plaćanje je takođe zamišljeno kao kripto prenos sredstava sa adrese klijenta na adresu agenta. Sve je to omogućeno pomoću ETH kriptovalute.

4.1 KONFIGURACIJA SISTEMA I KORIŠĆENI ALATI

Kako bi BPM bio upotrebljiv i ilustrativan, za njegovo modelovanje korišćen je *Camunda Modeler*, koji koristi BPMN (eng. *Business Process Model and Notation*) notaciju za modelovanje procesa.

BPMN je grafički prikaz za specifikaciju poslovnih procesa u modelu poslovnog procesa. Prvobitno je razvijen od strane Inicijative za upravljanje poslovnim procesima (eng. *Business Process Management Initiative* – BPMI), dok sada BPMN održava *Object Management Group* – OMG), otkako su se ove dve organizacije spojile 2005. Verzija 2.0. objavljena je u januaru 2011. godine i u tom trenutku je izmenjen i naziv u BPMN kako bi održavao uvođenje semantike izvršenja, koja je uvedena zajedno sa postojećim elementima notacije i dijagrama. Najnovija verzija BPMN-a je 2.0.2 koja je objavljena u januaru 2014. godine [4].

Korisnik preko *web* aplikacije popunjava date forme i ukoliko je funkcionalnost vezana za pametni ugovor, obraća se serverskoj strani *web* aplikacije. Server je povezan sa *Web3j* bibliotekom, koja pruža interfejs za laku interakciju sa *Ethereum* blokčejnom i njegovim čvorovima. Drugim rečima, web3j olakšava međusobnu komunikaciju između klijenta i *Ethereum* blokčejna putem JSON-RPC.

Pametni ugovor je napisan korišćenjem jezika *Solidity* [5], objektno-orijentisanog jezika višeg nivoa, koji služi za pisanje pametnih ugovora. Pametni ugovori suštinski predstavljaju male programske celine koje upravljaju ponašanjem naloga na *Ethereum* platformi. Na *Solidity* su uticali jezici kao što su C++, Python i JavaScript, a dizajniran je zarad upotrebe *Ethereum Virtual Machine* (EVM). EVM se može posmatrati kao analog JVM (*Java Virtual Machine*), ali koja koristi mrežu čvorova za komunikaciju. Ekstenzija fajla koji sadrži pametni ugovor je *.sol.*

S obzirom na to da je serverska strana implementirana u *Java Spring* tehnologiji, bilo je potrebno konvertovati pametni ugovor *Solidity* fajla u Java klasu. To nam omogućava *Solidity* kompajler (*solc*), koji prevodi *.sol* fajl u *.abi (Application Binary Interface)* i *.bin* fajlove, koji se potom pomoću *web3j* biblioteke konvertuju u *.java* klasu. Ovako izvedena klasa sastoji se iz svih funkcija (*static* tipa) koje sadrži pametni ugovor, kao i ugrađenih funkcija za *deploy* i iščitavanje istog. Sve funkcije iz ove klase se mogu pozivati u aplikaciji uobičajeno, kako se inače radi u programiranju. *Solidity* se takođe se koristi i za interakciju sa Android aplikacijama.

Što se tiče testne mreže za komunikaciju sa *Ethereum* platformom, korišćen je *Kovan*. S obzirom na to da svaka transakcija koja se izvršava na blokčejnu naplaćuje, potrebno je dobaviti testne „novce" - *Ether*-e. U ovu svrhu korišćen je *Kovan Faucet* koja omogućava legitimnim programerima da dobiju određenu sumu *Ether*-a, koji nemaju tržišnu vrednost, već služe samo za

postavljanje i testiranje pametnih ugovora na *Kovan* mreži.
Prilikom slanja zahteva za dodelu ovih sredstava potrebno je uneti adresu naloga, npr. 0xf3e6721B0974fDd801F74f59f584cEE9424D476d, odnosno eksterni nalog, sa kog će se raditi *deploy* pametnog ugovora, te će posle određenog vremena (uglavnom je to oko 24h) stići na taj nalog predodređena suma *Ether*-a. *Kovan Faucet* sprečava zlonamerne programere da dobiju velike količine ETH, kako ih ne bi zloupotrebljavali. Dakle, ovakva vrsta „novca" služi samo u svrhe razvoja softvera, odnosno testiranja. Nakon što se dobije određena testna suma kriptovalute, mogu se izvšavati transakcije na *Ethereum* platformi.
Za detaljan prikaz transakcija na blokčejnu, korišćen je *Etherscan* sajt koji poseduje spisak svih transakcija koje je izvršila određena adresa, odnosno sva plaćanja, kreiranje pametnih ugovora, kao i njihovo iščitavanje.

5. ZAKLJUČAK

Ovaj rad imao je za cilj da pokaže mogućnost korišćenja blokčejn tehnologije kao posrednika u komunikaciji poslovnih procesa. Blokčejn tehnologija je trenutno izuzetno uzbudljiva: ona ima potencijal ne samo da transformiše postojeće procese već i stvara nove mogućnosti i inovacije. Kako se pomamnost oko tržišta kriptovaluta smiruje, očekujemo da će preduzeća obraćati više pažnje na aplikacije i mogućnosti blokčejn tehnologije u industrijama kao što su nekretnine, finansije, zdravstvo i proizvodnja i ostalo.

Kao primer aplikacije koja je razvijana upotrebom blokčejna, tačnije *Ethereum*-a, prikazana je implementacija procesno bazirane aplikacije za iznajmljivanje automobila tzv. *Rent a car*. S obzirom na to da su korisnici ovakvog sistema nepoverljive strane, bio bi im potreban određeni autoritet, posrednik koji bi garantovao da se ispune sve obaveze između njih. Međutim, u ovom rešenju upravo tu ulogu preuzima Blokčejn, koji na svojoj platformi nudi mogućnost sklapanja elektronskih - pametnih ugovora. Budući da su zasnovani na kodu, pametni ugovori se mogu odmah i automatski izvršiti, bez oslanjanja na ručni prenos ili intervenciju instituta. Svaka ugovorna strana upisuje određene stavke koje joj odgovaraju, ukoliko ih druga potvrdi, ugovor se izvršava. Svaka transakcija koja je nastala prilikom upisivanja stavke u ugovor košta minimalno, dok bi notari i ostali posrednici naplatili mnogo veće sume novca za isti posao. Zatim, svaka stavka koja je upisana u pametni ugovor se ne može promeniti, te je vrlo teško doći do prevare neke od ugovornih strana.

Potencijalna unapređenja trenutnog rešenja:

1. Poboljšanje na UI strani, kako bi UI elementi bili što više *user-friendly*.
2. Što se tiče poslovnog procesa, bilo bi dobro razdvojiti svaki proces u zasebne module, pa ih pozivati iz kontrolonog kao podprocese.
3. Na *backend* strani može se unaprediti skalabilnost sistema, odnosno proširivost, ukoliko bi bilo još dodatnih ugovornih strana.
4. Što se tiče obaveštavanja klijenta o isteklom periodu najma, možemo implementirati sistem notifikacija, npr. podsetnik da treba automobil da se vrati.
5. Integrisati *web* aplikaciju kao deo celokupnog sistema za određenu kompaniju za iznajmljivanje automobila.

6. LITERATURA

[1] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System", http://www.bitcoin.org/, 2009.
[2] Decker, G., Kopp, O., Leymann, F., Pfitzner, K., & Weske, M.Decker, G., Kopp, O., Leymann, F., Pfitzner, K., & Weske, M. *Modeling Service Choreographies Using BPMN and BPEL4Chor. Lecture Notes in Computer Science*
[3] Ethereum Whitepaper https://ethereum.org/en/whitepaper/
[4] BPMN https://www.omg.org/spec/BPMN/2.0.2/
[5] Solidity language https://docs.soliditylang.org/en/v0.8.4/

Kratka biografija:

Zorka Jocović rođena je u Bijelom Polju 1995. god.
Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Primenjene računarske nauke odbranila je 2021.god.
kontakt:
zorkajocovic@yahoo.com