UDC: 004.7 Info M str. 4-10

OSNOVE FUNKCIONISANJA HYPERLEDGER FABRIC BLOCKCHAIN MREŽE
INTRODUCTION TO BLOCKCHAIN HYPERLEDGER FABRIC NETWORK

Lazar Lukić, Ivana Jovičić

REZIME: Blockchain je postala disruptivna tehnologija današnjice kako u životima krajnjih korisnika tehnologije, najčešće kroz kriptovalute, tako i kod ljudi koji razvijaju softver. Rezultat ovoga je pojavljivanje brojnih framework-a za razvoj sistema zasnovanih na blockchain arhitekturi. Najveći deo pažnje u ovom radu biće posvećen pregledu osnovnih koncepata jednog takvog framework-a koji se zove Hyperledger Fabric. Razlog razmatranja pomenutog framework-a jeste činjenica da je Hyperledger Fabric jedan od najzrelijih i najkompletnijih tehnologija za razvoj blockchain rešenja. Razmatraćemo osnovne koncepte, terminologiju kao i uloge članova Hyperledger Fabric mreže. Takođe upoznaćemo se sa osnovnim konceptima blockchain tehnologije.

KLJUČNE REČI: Blockchain, Hyperledger fabric, smart contract, chaincode

ABSTRACT: Blockchain has become the disruptive technology in today's world, in the lives of end-users of technology most commonly through cryptocurrencies, as well as for people who develop software. The result is the emergence of numerous frameworks for the development of systems based on blockchain architecture. Most of the attention in this paper will be a review of basic concepts of such framework that is called Hyperledger Fabric. One of the key reasons for considering mentioned framework in this paper is that Hyperledger Fabric is one of the most mature and most complete technologies for the development of blockchain based systems. Moreover, in this paper, we will consider basic concepts, the terminology and the role of members of the Hyperledger fabric network. We will also grasp basic concepts of blockchain technology

KEY WORDS: Blockchain, Hyperledger fabric, smart contract, chaincode

1. UVOD

Kako bi ceo privredni sistem funkcionisao pravilno i u skladu sa zakonom, potrebno je da postoji kontrola od strane centralnih autoriteta kojima fizička i pravna lica veruju i koja će obezbediti poštenu i pouzdanu razmenu informacija, dobara i slično.

Tako na primer, kad je reč o prenosu novčanih sredstava sa računa na račun, potrebno je izvršiti proveru samih učesnika transakcije i da li su oni platno sposobni da takvu transakciju obave. U ovom slučaju proveru validnosti učesnika i kontrolu same transakcija vrše banke. Banka je autoritet kome korisnici ukazuju poverenje i veruju da će banka pravilno obaviti svoj deo posla i da će se svaka transakcija obaviti u skladu sa pravilima.

Takođe, pored pomenutog tipa novčanih transakcija, sve popularnija je digitalna ekonomija koja obuhvata čitav dijapazon oblika plaćanja i transakcija koje su opet bazirane na poverenju prema nekom centralnom autoritetu. Korisnicima je potrebno da budu sigurni da će se željena razmena i plaćanje izvršiti, ali podjednako je bitno i da korisnik zna ko i kako upravlja njegovim podacima.

Kada su u pitanju servisi koji upravljaju korisničkim podacima, kao što je Facebook, korisnik mora da zna na koji način servis, čije usluge koristi, može da upotrebljava njegove podatke u neke dalje svrhe. Sve češći je slučaj da ovakav tip servisa prodaje podatake korisnika online biznisima radi boljeg i preciznijeg targetiranja korisnika na društvenim mrežama. Potrebno je da korisnici budu svesni da ovi servisi mogu biti maliciozni i neodgovorni. Ta malicioznost i neodgovornost se pre svega ogledaju u odnosu prema korisničkim podacima, prikupljanjem i upotrebom podataka u dalje svrhe bez korisničkog znanja i bez mogućnosti da korisnik dobije uvid u njih. Pomenuti problemi poverenja, transparentnosti i anonimnosti podataka su samo neki od problema koje primena blockchain tehnologije može rešiti.

Blockchain se koristi za digitalni zapis transakcija. Sam naziv potiče od njegove strukture gde su svi zapisi, koji se nazivaju blokovima, povezani u listu, koja se naziva lanac, tj. chain. Svaka transakcija dodata u blockchain sistem je validirana od strane više različitih učesnika mreže. Na taj način, uvodjenjem decentralizacije sistema i procesa konsenzusa između učesnika u blockchain mreži, rešava se problem poverenja koji je sve prisutniji. U ovakvom sistemu, nije dovoljno da jedan učesnik potvrdi validnost neke transakcije, već se kroz procese konsenzusa donosi odluka o prihvatanju ili odbacivanju transakcija, što eliminiše ulogu jednog centralizovanog autoriteta od poverenja. [1]

Jedan od glavnih elemenata blockchain tehnologije je distribuirana baza podataka, glavna knjiga (eng. *ledger*) svih transakcija koje su se izvršile između učesnika. Sve zapisane informacije na blockchain-u su trajne, tj. nemoguće ih je obrisati, a to obezbeđuje mogućnost revizije svih podataka, transakcija i interakcija između učesnika. Na ovaj način je pruženo rešenje problema transparentnosti ali ujedno i anonimnosti, jer nisu svi podaci dostupni svim učesnicima. Više reči o osnovnim konceptima blockchaina biće u drugoj sekciji ovog rada, gde će se razmatrati i tehnički aspekti ove tehnologije.

U okviru treće sekcije biće dat pregled različitih vrsta blockchain mreža, dok će u četvrtoj sekciji biti ukratko prikazana istorija Bitcoin-a i način njegovog rada.

Sekcija pet predstavlja srž ovog rada a to je uvod u Hyperledger Fabric, modularni blockchain framework koji služi kao osnova za razvoj blockchain rešenja i aplikacija. Pre svega će biti izloženi i detaljnije objašnjeni osnovni koncepti i terminologija, ali i sama arhitektura tehnologije i njeni učesnici.

Poslednja sekcija predstavlja rezime ovog rada.

2. BLOCKCHAIN TEHNOLOGIJA

Blockchain tehnologija predstavlja deljenu, transparentnu, distribuiranu, sinhronizovanu bazu podataka (eng. *ledger*) od poverenja. Distribuiranost je postignuta razvijanjem baze podataka na takozvanoj *peer-to-peer* (P2P) mreži uređaja. Čvor (eng. node) može biti bilo koji aktivan elektronski uređaj (npr. računar ili mobilni telefon) koji ima pristup internetu i svoju IP adresu. Svaki učesnik mreže, čvor, poseduje sopstvenu kopiju baze u kojoj se čuvaju izvršene transakcije (eng. *transactions*) između učesnika mreže. Kako vlasnici čvorova dobrovoljno daju resurse svog uređaja na korišćenje, omogućeno im je da prikupljaju proviziji od transakcija (eng. *transaction fees*) i na taj način zarade.

Transakcije se grupišu u blokove (eng. *blocks*) i čuvaju se od stvaranja mreže pa do sadašnjeg trenutka, bez mogućnosti da se brišu. Prvi kreirani blok se naziva *genesis block* i to je jedini blok u blockchain mreži koji nema "roditeljski" blok. Svi ostali blokovi sadrže adresu prethodnog bloka i na taj način je mreža struktuirana u vidu jednostruko spregnute liste blokova, odakle i potiče sam naziv ove tehnologije. Adrese preko kojih su povezani blokovi predstavljaju kriptografski potpisanu vrednost različitih elemenata bloka. O strukturi bloka će biti više reči u nastavku.

Da bi transakcija bila zapisana i sačuvana potrebno je da bude validirana i potvrđena od strane učesnika mreže korišćenjem kriptografije (eng. *cryptography*) i postizanjem konsenzusa (eng. *consensus*). Pomoću algoritma konsenzusa (eng. *consensus algorithm*) se definišu "pravila igre", tj. način na koji će učesnici mreže doći do dogovora oko validacije transakcije. Najčešće korišćen algoritam je *Proof of Work* (PoW) koji funkcioniše po principu da što više posla čvor odradi, veće su šanse da će moći da validira transakciju i učestvuje u kreiranju sledećeg bloka i na taj način ostvari nagradu. [2]

Kriptografija (eng. *cryptography*) u blockchain sistemu se koristi u svrhu zaštite identiteta učesnika transakcije, kao i za osiguravanje samih podataka transakcije kako oni ne bi mogli biti izmenjeni. Svaki blok kreira svoju adresu preko koje će biti povezan sa narednim blokom tako što primenjuje hash funkciju na svoje određene elemente, korišćenjem SHA256 algoritma. Hash funkcija predstavlja funkciju koja za dati ulazni tekst proizvoljne dužine vraća hash vrednost fiksne dužine, odnosno predstavlja izlaz nepovratne matematičke funkcije. Hash funkcije su determinističke, što znači da za isti ulaz uvek dobijamo isti izlaz. Takođe mala promena ulaza treba da promeni dobijen izlaz, odnosno hash vrednost, čime se izbegava zavisnost između dobijenih rezultata. Kako se transakcije unutar bloka čuvaju u vidu hash vrednosti koja predstavlja izlaz hash funkcije, a adresa bloka se kreira takođe pomoću hash funkcije, najmanja izmena transakcije, dovodi do totalno različite vrednosti hash-a bloka, a samim tim i adresa prethodnog i sledećeg bloka u tom lancu. Ako bi neko hteo da izmeni vrednost transakcije unutar bloka, morao bi da izračuna nove hash vrednosti svih blokova u lancu. [3]. Na ovaj način je korišćenjem kriptografije, distribuiranosti mreže i algoritma konsenzusa postignuta imutabilnost blockhain-a, odnosno nemogućnost izmene podataka.

Kada je u pitanju zaštita identiteta učesnika, ona se postiže upotrebom kriptografske kombinacije javnog i privatnog ključa (eng. *Public and Private Key*). Naime, svaki učesnik mreže je jedinstveno identifikovan svojim javnim ključem koji je dostupan ostalim učesnicima kako bi bila omogućena komunikacija između njih. Sa druge strane, privatni ključ ostaje samo kod svog vlasnika i koristi se za potpisivanje transakcije kako bi ostali učesnici bili sigurni da je transakcija inicijalizovana od strane ispravnog učesnika. [4]

Što se tiče same strukture bloka, svaki blok se sastoji od zaglavlja i liste transakcija. Zaglavlje sadrži meta podatke kao što su:

1. Hash vrednost prethodnog bloka
2. Trenutno vreme
3. Nonce - proizvoljan kriptografski broj koji se može iskoristiti samo jednom i koji se koristi kako bi varirao ulaz u hash funkciju i na taj način onemogućilo predviđanje izlaza funkcije.
4. Verzija bloka
5. Hash vrednost korena Merkleovog drveta (eng. *Merkle root*) koja se koristi pri validaciji transakcija jer je Merkelovo drvo zapravo hash vrednost od hash vrednosti svih transakcija iz bloka.

Glavne prepoznate prednosti blockchain-a su:

● Bezbednost

Dobro dizajnirana blockchain mreža je znatno pouzdanija od tradicionalnih, centralizovanih baza podataka. Sigurnost se ogleda kroz činjenice da svaki učesnik mreže ima svoju kopiju baze i da je zbog objašnjenog načina povezivanja blokova, praktično nemoguće izmeniti sadržaj transakcija i baze.

● Transparentnost

Jednostavna dostupnost podacima se pokazala kao značajna prednost u mnogim privrednim sektorima: investitori mogu da prate kretanje svog novca, javne ustanove lakše upravljaju dokumentima, pojedinci prate svoje podatke i novčane transakcije itd.

● Elastičnost

Elastičnost blockchain arhitekture se ogleda u prilagodljivosti različitim oblicima napada. S obzirom da je reč o velikom broju učesnika sa svojim kopijama baze, i da je neophodna validacija i konsenzus da bi transakcija bila potvrđena, sve dok je bar nekoliko učesnika otporno na napad, podaci su sigurni. [5]

3. TIPOVI BLOCKCHAIN MREŽA

Iako sve blockchain mreže imaju neke zajedničke karakteristike kao što su decentralizovanost, konsenzus i garancija neizmenjenosti transakcija, ipak postoji više tipova blockchain mreža. Osnovna podela blockchain mreža je na javne i privatne.

Javne blockchain mreže (eng. *Public Blockchains*) predstavljaju mreže kod kojih je ulazak novih korisnika otvoren, odnosno svako može da učestvuje i svi učesnici su anonimni. Učesnici javnih blockchain mreža dolaze do generalnog dogovora, konsenzusa, o usvajanju novog bloka transakcija primenom *proof of work* algoritma. Proof of work proces verifikacije transakcija predstavlja određenu količinu posla koju član mreže mora da odradi kako bi dokazao validnost transakcija, a

reč je o poslu koji je jako obiman i intenzivan. Iz ovog razloga proof of work je zapravo spor proces i resursno proždrljiv.

Jedna od prednosti ovog tipa blochchain mreže je činjenica da nema troškova infrastrukture. Nema potrebe za administracijom sistema i održavanjem servera jer se koristi decentralizovni sistem. [6] Takođe, prednost javne blockchain mreže je i široka dostupnost i jednostavnost korišćenja od strane velikog broja entiteta, bez potrebe učešća treće strane kako bi se izvršila verifikacija.

Primena: kriptovalute kao što su Bitcoin, Ethereum, Monero, Litecoin, Dodgecoin...

Privatna blockchain mreža (eng. *Private Blockchain*) je blockchain mreža gde je identitet svakog učesnika poznat i kriptografski autentifikovan tako da može biti zapisano i ispraćeno ko je izvršio koju transakciju. Takođe, prisutan je mehanizam kontrole kojim se definiše ko ima dozvolu da čita i zapisuje podatke, ko može da izaziva transakcije i ko je zadužen za upravljanje učesnicima mreže. Upravo ovo pruža visok nivo zaštite i privatnosti podataka. [7]

Ovaj tip mreže koristi prednosti blockchain tehnologije tako što definiše tačnu grupu učesnika koji će vršiti verifikaciju transakcija. Na ovaj način se smanjuju troškovi transakcije jer se verifikacija vrši na manjem broju korisnika nego što je situacija kod javnih mreža. Ujedno se smanjuje i mogućnost od takozvanog napada većine (eng. *Majority attack*) gde napadač treba da poseduje minimum 51% resursne moći mreže, što bi mu omogućilo da plasira lažne transakcije jer bi vršio pravljenje bloka brže od ostatka mreže. [8]

Primena: Blinking, MONAX, Multichain…

4. PRVA USPEŠNA REALIZACIJA BLOCKCHAIN TEHNOLOGIJE - BITCOIN

Blockchain tehnologija je zaživela kroz realizaciju prve kripto valute na svetu pod imenom Bitcoin (BTC). Tvorac Bitcoin-a, 2008. godine objavljuje naučni rad pod nazivom „Bitcoin: Peer-To-Peer Electronic Cash System". Individua ili grupa koja objavljuje ovaj naučni rad se predstavlja pod imenom Satoši Nakamoto. U pomenutom radu Bitcoin je definisan kao "potpuna peer-to-peer verzija elektronskog keša koja omogućava direktan prenos sredstava između korisnika bez posredovanja finansijske institucije". [9] Satoši u svom radu navodi da je potreban sistem za elektronsko plaćanje koji je baziran na kriptografskom dokazu, umesto na poverenju, koji omogućava učesnicima da razmenjuju sredstva bez trećeg lica kojem veruju. Ideja je u potpunosti realizovana i u današnje vreme je ljudima omogućeno da vrše plaćanja i transfere novca korišćenjem upravo Bitcoin-a.

Kao što je navedeno, Bitcoin je zasnovan na blockchain tehnologiji i infrastrukturi javnog ključa (eng. *Public key infrastructure* - PKI). U infrastrukturi javnog ključa korisnik ima par ključeva, javni i privatni. Javni ključ predstavlja adresu Bitcoin novčanika (eng. *Wallet*), a njegovo posedovanje omogućava korišćenje novčanika i učestvovanje u manipulaciji sredstvima. Privatni ključ se koristi za autentifikaciju korisnika. Naime Bitcoin novčanik korišćenjem privatnog ključa potpisuje transakciju, pružajući matematički dokaz da je transakcija zaista došla od vlasnika novčanika. [10]

Svaka transakcije se sastoje od javnog ključa pošaljioca, javnih ključeva primaoca i vrednosti koja se prenosi. U skladu sa blockchain tehnologijom, transakcija se upisuje u blok (na deset minuta), a novi napravljen blok se povezuje sa prethodnim blokom. Svi blokovi i sve transakcije ikada napravljene na Bitcoin mreži se čuvaju na diskovima korisnika koji predstavljaju čvorove mreže, a to omogućava čvorovima da proveravaju validnost svake nove transakcije korišćenjem prethodnih blokova. Čvorovi dobijaju određenu količinu Bitcoin novčića za ovaj procesno intenzivan zadatak. Metod ove provere se naziva rudarenje (eng. *Mining*), što je jedan od načina da se zaradi ova kriptovaluta. Sama provera validnosti transakcije se vrši korišćenjem algoritma Proof-of-Work.

Jedna od glavnih i najočiglednijih prednosti Bitcoin-a je njegova **nezavisnost** od vlasti i državnih autoriteta koje kontrolišu transakcije, uvode takse, poreze i slično. O njegovoj nezavisnosti govori i činjenica da je **lako prenosiv** jer je potpuno digitalan. Naime, može se čuvati onlajn ili preneti putem npr. usb-a, bez obzira o kojoj svoti novca je reč, a transakcije se vrše bez posrednika.

Takođe, upravljanje transakcijama je u potpunosti u rukama korisnika, tj. vlasnika bitcoin-a. Niko ne može izvršiti transakciju bez odobrenja, a novac se može i dodatno zaštiti rezervnim kopijama i šifrovanjem. Pored navedenog, **sigurnost i kontrola** se ogledaju i u činjenici da se identitet korisnika nikad ne otkriva, i da je zaštićen pri svakoj transakciji. Nasuprot nedostupnosti podataka samih korisnika, podaci o pojedinačnim transakcijama su **transparentni** i dostupni u realnom vremenu. Međutim, BTC protokol je šifrovan, a blockchain mreža je decentralizovana što onemogućava da ga neki pojedinac kontroliše ili upravlja njime.

Naravno, pored navedenih pozitivnihi strana Bitcoin-a, prisutne su i negativne, otežavajuće strane. Jedna od njih je pravni status koji se razlikuje od države do države. Neke uzimaju u obzir njegove prednosti i podstiču njegovu upotrebu, dok su druge zabrinute i smatraju ga nelegalnim sredstvom plaćanja. Postojanje različitih 'deep-web' tržišta koja primaju samo BTC podstiče nezakonitu trgovinu što je alarm nekim vlastima da zabrane njegovu upotrebu.

Što se tiče vrednosti samog novca, reč je **nestabilnoj** valuti čija cena drastično varira i prolazi kroz faze koje se nazivaju "mehurima" i krahovima.

Bitcoin danas predstavlja jednu od najkontraverznijih tehnologija. Trenutna vrednost svih Bitcoina koji su u cirkulaciji na mreži iznosi preko 147 milijardi dolara [20]. Kontraverznost se sastoji u anonimnosti Bitcoin transakcija. Anonimnost koja je jedna od glavnih prednosti ove tehnologije, omogućava i crno tržište, odnosno trgovinu oružijem, narkoticima, ljudima. Ipak Bitcoin opstaje uprkos svojim negativnim aspektima, jer predstavlja validnu i dostojnu zamenu za tradicionalne valute. [11]

5. HYPERLEDGER FABRIC

Hyperledger fabric (HLF) predstavlja framework napravljen u vidu softvera otvorenog koda za razvoj distribuiranih, zaštićenih blockchain sistema, tj. nudi gotovo softversko rešenje za izgradnju distribuiranih aplikacija.

HLF je tehnologija distribuirane glavne knjige (eng. *distributed ledger technology* - DLT) i jedan je od projekata Linux fondacije. Kao osnov za razvoj rešenja sa modularnom arhitekturom, Hyperledger Fabric omogućava da se komponente kao što su konsenzus, distribuirana glavna knjiga, provajder članstva i slično, menjaju i modifikuju po takozvanom principu *plug-and-play,* što znači da komponente rade nezavisno jedne od drugih. [12] Ovaj oblik modularnosti pruža privatnost, otpornost, ali i prilagodljivost i mogućnost proširenja u zavisnosti od potreba specifičnog biznisa.

Glavna razlika Hyperledger fabric-a u odnosu na druge blockchain framework-e jeste mogućnost podele odgovornisti i uloga učesnika mreže. Podela odgovornosti omogućava modularnost i bolje performanse. Za razliku od drugih blockchain sistema gde se pametni ugovori izvršavaju na svim čvorovima, u HLF izabrani podskup čvorova može da izvršava pametni ugovor. Izvršavanje pametnog ugovora na podskupu čvorova mreže, omogućava potencijalno paralelno izvršavanje. Takođe, HLF predstavlja prvi blockchain sistem koji omogućava pisanje pametnih ugovora (eng. *smart contract*) u programskim jezicima opšte primene kao što su Java, Go i Node.js, dok druge platforme zahtevaju pisanje pametnih ugovora u domenski specifičnom jeziku za tu platofmu. Korišćenje standardnih programskih jezika omogućava šire i jednostavnije usvajanje među programerima.

5.1 *HLF framework arhitektura*

S obzirom da je reč o blockchain sistemu, Hyperledger fabric mreža se sastoji od velikog broja učesnika, čvorova mreže (eng. *peers*), koji komuniciraju jedni sa drugima. Izvršavanjem programa koji se nazivaju chaincode-ovi upravlja se podacima i menja se stanje baze podataka, tj. glavne knjige (eng. *ledger*). Chaincode predstavlja softverski kod koji kada se izvrši ostavlja trag promene stanja u vidu transakcije (eng. *transaction*). Transakcije moraju biti izvršene, potvrdjene (eng. *endorsed*), zatim i odobrene i samo takve transakcije mogu imati uticaj na promenu stanja.

Čvorovi su komunikacioni entiteti blockchain mreže. Sam naziv čvor ima samo logički kontekst jer više čvorova može biti pokrenuto na istom fizičkom serveru. Tri osnovna tipa čvorova su:

1. Klijent (eng. *client* ili *submitting-client*) je čvor koji ima ulogu entiteta koji deluje u ime krajnjeg korisnika. Ovaj čvor, od krajnjeg korisnika sisetema, dobija zahtev za izvršenje određene akcije, konektuje se na čvorove mreže i poziva zahtevanu akciju. Nakon dobijenog odgovora šalje zahtev za odobrenje transakcije do ordering servisa i šalje odgovor nazad korisniku.
2. Peer-ovi su čvorovi koji održavaju stanje glavne knjige tako što dobijaju blokove transakcija od ordering servisa i potvrđuju ih. Peer može imati specijalnu ulogu endorsing čvora i tada je on zadužen i za izvršenje određenog chaincode-a.
3. Orderer čvor je čvor koji izvršava komunikacioni servis koji obezbeđuje garanciju isporuke blokova i zapisivanja transakcija.

HLF uvodi koncept **kanala** (eng. *channel*) koji je zapravo logička struktura i predstavlja vid "privatne" podmreže između dva ili više čvora. Na ovaj način se omogućava da komunikacija unutar kanala bude izolovana i zaštićena. Transakcije i podaci na kanalu su vidljivi samo članovima kanala. [7]

Čvorovi mreže se logički grupišu i u **organizacije** (eng. *organizations*). HLF mreža je izgrađena od čvorova koji pripadaju različitim organizacijam koje učestvuju u sistemu i poslovanju. Čvorovi različitih organizacija mogu biti na istom kanalu.

Pametni ugovori (eng. *smart contrac)* ili **chaincode**-ovi, kako su nazvani u HLF-u, su programi koji su instalirani na čvorovima i sadrže biznis logiku sistema. Koriste se za upravljanje podacima i izvršavanje samih transakcija. Mogu biti napisani u programskim jezicima Java, Go ili Node.js.

Postoji nekoliko tipova **transakcija** u Hyperledger fabric-u:

1. Deploy transakcije - koje se koriste za instaliranje chaincode-a na mrežu
2. Invoke transakcije - koje su uslovljenje deploy transakcijama, jer uz pomoć invoke transakcija pozivamo određene funkcije na chaincode-u, koje mogu a ne moraju da promene stanje.
3. Read-only transakcije - koje ne ostavljaju trag na ledger-u već predstavljaju samo čitanje podataka.
4. Cross-chaincode transakcije - pomoću kojih pozivamo iz jednog chaincode-a funkcije drugog. [13]

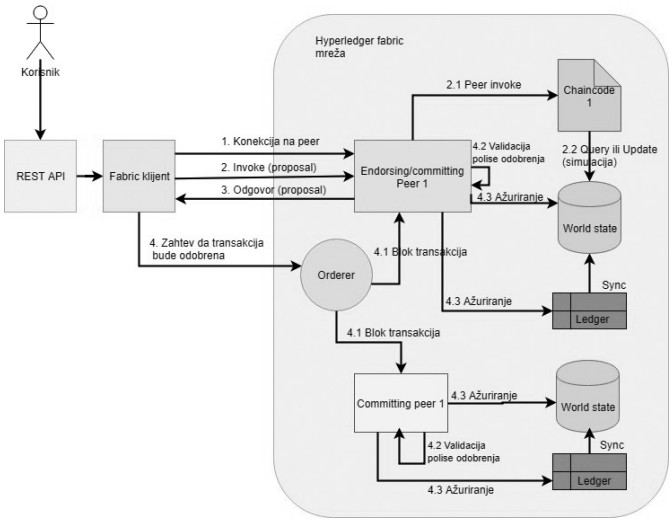
Glavna knjiga (eng. *ledger*) beleži stanje podataka i transakcija i svaki čvor mreže ima repliciranu kopiju glavne knjige. Podaci se čuvaju u strukturi ključ-vrednost (eng. *key-value*). Glavna knjiga se satoji od dve komponente:

1. Baza stanja sveta (eng. *world state*) - baza koja sadrži trenutne vrednosti podataka iz glavne knjige. Korisna je zbog brzog i jednostavnog pristupa trenutnim vrednostim, umesto da se pretražuju čitavi logovi transakcija. Stanje ove baze se često menja jer se podaci konstantno kreiraju, ažuriraju i brišu. Kako se podaci čuvaju u ključ-vrednost strukturi, za bazu stanja sveta koriste se takozvane NoSQL baze podataka koje su zasnovane na dokumentima i ključ-vrednost strukturama. Konketno, koristi se CouchDB ili LevelDB. Pri izvršavanju chaincode-a uzimaju se vrednosti iz baze stanja sveta. Razlog ovoga je da bi interakcije chaincode-a bile efikasnije i performantnije.
2. Blockchain - log transakcija koji beleži sve promene nad bazom stanja sveta. Transakcije su grupisane u blokove koje se dodaju na lanac blokova. Jednom zapisani, podaci ove komponente se ne mogu menjati i brisati.

Osnovna paradigma HLF-a je *execute-order-validate* [14]. Paradigma se sastoji iz tri dela: (1) izvršavanje (eng. *executing*) transakcije u bilo kom redosledu, moguće je i paralelno izvršavanje (2) *ordering* kroz protokol konsenzusa. (3) potvrđivanje (eng. *validation)* transakcija.

Svi čvorovi prolaze kroz fazu potvrđivanja, tj. svaki čvor validira transakciju i ažurira glavnu knjigu. Međutim, ne prolaze svi kroz fazu izvršavanja. HLF uvodi koncept **politike odobravanja** (eng. *endorsment policy*) kojom se definiše koji čvorovi moraju izvršiti transakciju, a zatim se i složiti oko rezultata pre nego što je transakcija zapisana. HLF pruža i mali domenski specifičan jezik kojim se definiše sama politika odobravanja. Primer politike odobravanja je da je definisano da čvor A, B i C moraju izvršiti transakciju tipa T ili da najmanje tri čvora iz kanala F moraju izvršiti transakciju tipa P. [15]

Execute-order-validate proces će detaljnije biti objašnjen u nastavku uz pomoć slike 1.

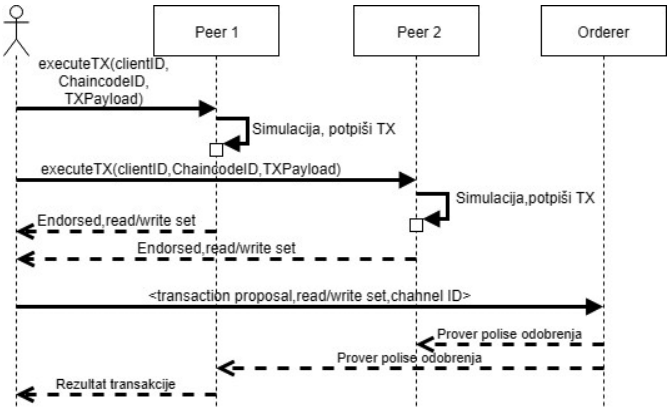


Slika 1 - *Simbolički prikaz Hyperledger fabric mreže*

Na Slici 1 vidimo komunikaciju između aplikacije i članova mreže na visokom nivou. Aplikacija se konektuje na čvor (korak 1.) i autorizovana je da vrši interakciju sa mrežom. Kao što se može videti na slici, aplikacija poziva čvor da izvrši akciju (korak 2.). Čvor koga poziva aplikacija da izvrši simulaciju se naziva *endorsing peer* koji predstavlja člana u mreži koji izvršava chaincode. Endorsing peer takođe ima dodatnu ulogu validacije polise odobrenja (eng. *endorsment policy*) koja predstavlja predefinisani skup odobrenja i pravila (eng. *endorsement*) koja moraju biti zadovoljena. Pozvana akcija za izvršavanje može biti npr. čitanje ili upisivanje odnosno neka izmena. Ova akcija se naziva predlog za izvršenje (eng. *proposal*). Čvor zatim poziva odgovarajući chaincode (korak 2.1.). Nakon što endorsing čvor izvrši chaincode, on daje odobrenje (eng. *endorsment*) da je izvršio pametni ugovor. Ovim procesom on ostavlja svoj digitalni potpis, kako bi se identifikovalo koji je tačno čvor iz naše mreže izvršio chaincode i da nije neki maliciozni. Odgovor se vraća do aplikacije (korak 3.) koja zatim zahteva da transakcija bude odobrena (korak 4.). Zahtev za odobrenje transakcije se šalje čvoru u mreži koji se naziva *orderer* ili *ordering service*. Uloga orderer-a je da validira transakcije, napravi blok transakcija i pošalje taj blok svim relevantnim endorsing i commiting čvorovima u mreži (korak 4.1.). *Committing peer* predstavlja čvor u mreži koji samo vrši validaciju polise odobrenja. Nakon validacije polise odobrenja (korak 4.2.) endorsing i committing čvorovi vrše ažuriranje glavne knjige i baze stanja sveta (korak 4.3.).

5.2 *Kako se odobravaju transakcije u HLF?*

Sam proces odobravanja transakcija možemo ilustrovati kroz primer. Recimo da imamo situaciju u kojoj jedan korisnik želi da prebaci određenu količinu novčića nekom drugom korisniku. Logika transfera novčića nalazi se u pametnom ugovoru, a funkcija koja vrši ovo prebacivanje zahteva adresu pošiljaoca, adresu primaoca i količinu novčića. Korisnik šalje zahtev aplikaciji koja je povezana na mrežu da izvrši ovo prebacivanje. Aplikacija poziva odgovarajuće čvorove koji zatim pozivaju pametni ugovor i odgovarajuću funkciju u njemu. Nakon izvršavanja, aplikacija prikuplja odgovore od čvorova. Kao što smo već objasnili, ove je predlog i odgovor za izvršavanje koji još uvek nema uticaj na glavnu knjigu. Pošto korisnik hoće da izvrši neku promenu, u ovom slučaju prebacivanje novca, potrebno je da ova transakcija bude validirana i da rezultat bude zapisan u glavnu knjigu kako bi ostao trag o svim transferima i promenama. Aplikacija šalje zahtev za odobrenje transakcije do orderer čvora. Orderer odobrava, pravi blok transakcija i šalje kreirani blok ostalim čvorovima kako bi ga oni dodali i upisali na ledger.



Slika 2 - *Tok odobravanja transakcija*

Detaljan tok odobravanja transakcije možemo videti na slici 2. Aplikacija koja je povezana sa mrežom, šalje *propose* poruku određenom skupu *endorsing* čvorova. Ova poruka predstavlja samo zahtev za izvršavanje. Poruka sadrži brojne paramete kao što su:

1. clientSig - potpis klijenta u vidu sertifikata
2. txPayload - sadrži argumente i funkciju koja se poziva u chaincode-u
3. ChaincodeID - predstavlja jedinstven ID chaincode-a na koga se poziv za izvršavanje odnosi.

Kada poruka stigne do endorsing čvora, on prvo proverava validnost clientSig. U slučaju da je validan, endorsing čvor simulira izvršavanje transakcije. Odnosno ovo izvršavanje još uvek nema efekat na ledger. Prilikom simulacije transakcije, endorsing čvor na osnovu chaincodeID-a poziva odgovarajući chaincode i pronalazi odgovarajuću funkciju kojoj prosleđuje argumente iz txPayload parametra. Nakon toga vrši se provera polise odobrenja i ukoliko je zadovoljena, čvor dodaje svoj digitalni potpis.

Rezultat izvršavanja se šalje aplikaciji koja je pozvala endorsing čvor. Aplikacija prikuplja onoliko odgovora od endorsing čvorova, koliko je potrebno da bi se zadovoljila polisa odobrenja. Ako je ovaj broj zadovoljen, transakcija se smatra odobrenom. Treba da imamo u vidu da je za sada transakcija samo odobrena, ali da još uvek nema efekta na bazu stanja ili ledger. Klijent zatim emituje poruku do ordering servisa. Poruka sadrži:

1. transaction proposal - rezultat prethodne faze gde je izvršen konkretan chaincode
2. read/write set - set podataka koji su čitani iz baze stanja i koji će biti upisani
3. ChannelID - predstavlja ID kanala na koga se chaincode odnosi

Nakon dodatnih provera orderer dodaje transakcije u blok. Transakcije unutar bloka se validiraju u odnosnu na polisu odobrenja, gde se takođe vrši dodatna provera kako bi se potvrdilo da nije bilo izmene na ledger-u u odnosu na read/write set svake transakcije. Transakcije postaju validne ili invalidne. Nakon toga, ordering service emituje svim čvorovima da treba da dodaju ovaj blok u lanac i read/write set se zapisuje u bazu stanja sveta.

5.3. *Identitet učesnika HLF mreže*

Kao oblik privatnog blockchain-a, HLF zahteva da svi učesnici mreže (čvorovi, orderer, klijentska aplikacija itd.) imaju svoj **digitalni identitet** kojim će se predstavljati u mreži kako bi se vršila provera sigurnosti komunikacije, kako bi se osiguralo da su poruke i akcije autentifikovane i slično.

Svaki učesnik mreže ima svoja dva kriptografski povezana ključa: **javni ključ** (eng. *public key*) koji je dostupan svim ostalim članovima i koristi se za potvrdu identiteta pošiljaoca poruke, i **privatni ključ** (eng. *private key*) koji se koristi za potpisivanje poruka i koji uvek ostaje samo kod svog vlasnika. Pošiljalac poruke svojim privatnim ključem potpisuje poruku, dok sa druge strane, u cilju da proveri autentičnosti poruke, primalac koristi javni ključ pošiljaoca koji je dostupan svim članovima mreže.

Za distribuciju kroz mrežu i autentifikaciju javnih ključeva koristi se infrastruktura javnog ključa (eng. *public key infrastructure* - PKI). PKI je skup internet tehnologija koje obezbeđuju da učesnici veruju jedni drugima i da komunikacija u mreži bude sigurna. PKI je baziran na mehanizmu koji se naziva **digitalni sertifikat** (eng. *digital certificate*). Digitalni sertifikat ili sertifikat javnog ključa se koristi kako bi se povezao javni ključ sa entitetom koji ga poseduje. Digitalni sertifikat se sastoji od javnog ključa koji se sertifikuje, ključnih identifikacionih podatka vlasnika javnog ključa, metapodataka samog sertifikata i digitalnog potpisa javnog ključa koji je napravljen od strane izadavaoca sertifikata. [16]

Sertifikati su u skladu sa standardom X.509 i kako bi bili validni moraju biti izdati od autorizovanog **autoriteta za sertifikate** (eng. *Certificate Authority* - **CA**). CA izdaje digitalne sertifikate i potpisuje ih svojim privatnim ključem. Ukoliko neki učesnik sistema veruje tom CA (i zna njegov javni ključ), on može da proveri CA potpis na izdatom sertifikatu. Ukoliko je potpis validan, on može da veruje i da je određeni učesnik zaista vlasnik javnog ključa koji je uključen u sertifikat. [13]

CA kao komponenta koja upravlja identitetima svih učesnika mreže i njenih korisnika koristi liste kontrole pristupa (eng. *access control list - ACL*). Ove liste olakšavaju praćenje prava pristupa korisnika i garantuju da je svaka transakcija izvršena od strane registrovanog korisnika. Takođe, pri proveri sertifikata koristi se i lista ukinutih sertifikata (eng. *certificate revocation list - CRL*) koja sadrži spisak opozvanih sertifikata koji više nisu validni i u upotrebi.

CA izdaje početni sertifikat (eng. root certificate - ***rootCert***) svakom članu (organizaciji ili pojedincu) koji je autorizovan da pristupi mreži. Takođe, izdaje i sertifikat upisa (eng. enrollment certificate - ***eCert***) svakom članu mreže, serverskoj aplikaciji i povremenim korisnicima. Svakom upisanom korisniku se izdaje i sertifikat transakcija (eng. transaction certificate - ***tCerts***). Svaki tCert odgovara jednoj transakciji u mreži. [17]

Određivanje koji CA je autorizovan i od poverenja za izdavanje sertifikata i definisanje članova domena kao što je npr. organizacija je zadataka komponente koja se zove Provajder članstva (***Membership Service Provider*** - *MSP*). MSP ima zadatak da izlista članove nekog domena (organizacije, kanala itd.), njihove uloge, privilegije pristupa, kao i CA servise koji su autorizovani da ovim članovima izdaju validne sertifikate.

MSP omogućava apstrakciju svih kriptografskih mehanizama i protokola iza izdavanja i validiranja sertifikata i autentikacije korisnika. HLF sistem može imati jedan ili više MSP-a. Jedan važan preduslov pre postavljanja instance MSP-a je da se njegova konfiguracija mora lokalno navesti na čvorovim mreže i orderer-u. Ovo će omogućiti čvorovima i ordereru da potpisuju poruke ali i da validiraju poruke i sertifikate drugih učesnika. [18]

5.4. *Prednosti i nedostaci Hyperledger Fabric-a*

Neke od prednosti Hayperldger Fabric platforme su:

● Privatna blockchain mreža

HLF mreža je privatna blockchain mreža gde je poznat identitet svih učesnika. U mnogim privrednim oblastima kao što je enkonomska ili zdravstvena industrija, neophodno je znati ko sve ima pristup podacima i kontrolisati pristup, što HLF u potpunosti omogućava.

● Povećan nivo poverenja

Činjenica da je proces izvršavanja transakcije podeljen u nekoliko faza i da svaka faza i svaki akter određene faze proverava i validira podatke i izvršioce, povećava nivo poverenja.

● Koncept kanala

Biznisi često imaju potrebu da pojedine podatke čuvaju posebno zaštićeno, bilo zbog zakona, regulativa o poverljivosti ili nekog drugog razloga. HLF to omogućava pomoću koncepta kanala gde zaštićeni podaci odlaze samo do članova kanala, tj. do učesnika koji smeju da im pristupe.

● Brzo pretraživanje podataka

Čuvanje podataka u strukturama ključ-vrednost i korišćenje baza podataka kao što su LevelDB ili CouchDB omogućava brzo pretraživanje i brz pristup podacima. [19]

Nedostaci ovakvog distribuiranog sistema proizilaze iz karakteristika koje sa druge strane donose benefite. Neki uočeni nedostaci su:

● Kompleksnost konfiguracije i otežano održavanje mreže

HLF sistem je zasnovan na blockchain arhitekturi. Veći broj učesnika distribuirane blockchain mreže zahteva kompleksniju konfiguraciju a to dodatno otežava sam proces upravljanja i održavanja mreže

● Povećani troškovi

Kako svi čvorovi imaju svoju kopiju baze podataka, izvršavaju chaincode-ove, validiraju transakcije i kriptografski proveravaju učesnike mreže, potrebna je velika količina računarske snage što direktno utiče na povećanje troškova.

● Mogućnost usporenosti

Zbog kompleksnosti sistema i samog procesa izvršavanja i odobravanja transakcija, nekad je potrebno više vremena dok krajnji korisnik sistema dobije odgovor.

6. ZAKLJUČAK

Blockchain tehnologija ima potencijal da reši kako probleme finansijskih transakcija, tako i različite probleme nefinansijske prirode kao što je na primer upravljanje korisničkim podacima. Kripto valute postaju sve zastupljenije, a krajnji korisnici sve jasnije vide prednosti i mogućnosti tehnologije kao što je blockchain.

Cilj blockchain tehnologije je da obezbedi anonimnost, sigurnost, privatnost i transparentnost podataka. Ove mogućnosti i karakteristike sve više biznis sistema prepoznaju kao priliku da unaprede svoj tradicionalni način poslovanja i pruže, kako svom sistemu, tako i krajnjim korisnicima veći nivo bezbednosti i kontrole. Hyperledger fabric framework omogućava i olakšava razvoj takvih rešenja i aplikacija zasnovanih na blockchain arhitekturi.

Hyperledger fabric je implementacija privatnog blockchain sistema gde je kontrolisan pristup samoj mreži što je posebno bitno za biznis aplikacije koje ne žele da podaci budu javno dostupni, kao što je to slučaj kod kripto valuta. Pored velikog broja prednosti HLF-a koje se ogledaju kroz performanse, bezbednost podataka, separaciju odgovornosti između učesnika i slično, potrebno je istaći i jedan vid jednostavnosti korišćenja. Naime, pametni ugovori se pišu u standardnim programskim jezima što omogućava programerima brži razvoj i mogućnost da veću pažnju usmere na implementaciju same biznis logike. Naravno, tu su i mane kao što su visoka kompleksnost konfiguracije i održavanja mreže, ali to su posledice karakteristika koje sa druge strane donose veće benefite korisnicima. Svakako je jasno da je Hyperledger fabric tehnologija novije generacije koja će tek pokazati sve svoje potencijale i mogućnosti.

7. LITERATURA

[1] "Blockchain." Tech Terms. Accessed July 2018. https://techterms.com/definition/blockchain.

[2] Kravchenko, Pavel. "What Is Consensus Algorithm in Blockchain and Why Do We Need It?" Cryptovest. June 28, 2018. Accessed July 2018. https://cryptovest.com/education/what-is-consensus-algorithm-in-blockchain-and-why-do-we-need-it/.

[3] "What Is Hashing? Under The Hood Of Blockchain." Blockgeeks. January 01, 1969. Accessed July 2018. https://blockgeeks.com/guides/what-is-hashing/.

[4] "How Cryptography Is Used in Blockchain?" Quora. Accessed July 2018. https://www.quora.com/How-cryptography-is-used-in-blockchain .

[5] "What Is A Blockchain? Introduction To Digital Ledgers." Crypto Briefing. September 11, 2018. Accessed July 2018. https://cryptobriefing.com/what-is-a-blockchain-digital-ledger/ .

[6] "Blockchains & Distributed Ledger Technologies." BlockchainHub. Accessed July 2018. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/ .

[7] Thakkar, Parth, Senthil N. Nathan, and Balaji Viswanathan. "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform." May 2018. Accessed July 2018. https://arxiv.org/pdf/1805.11390.pdf .

[8] "The 4 Types of Blockchain Networks Explained." The 4 Types of Blockchain Networks Explained - ILTA. Accessed July 2018. https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained?ssopc=1.

[9] Marr, Bernard. "A Very Brief History Of Blockchain Technology Everyone Should Read." Forbes. March 20, 2018. Accessed August 2018. https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#c00973e7bc47 .

[10] "How Does Bitcoin Work?" FAQ - Bitcoin. Accessed August 2018. https://bitcoin.org/en/how-it-works .

[11] "What Is Bitcoin? History, Characteristics, Pros and Cons." Cointelegraph. Accessed August 2018. https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin#how-to-get-bitcoin .

[12] "Hyperledger Fabric." Hyperledger. Accessed August 2018. https://www.hyperledger.org/projects/fabric .

[13] Hyperledger-fabric docs. Accessed August 2018. https://hyperledger-fabric.readthedocs.io/en/release-1.2/ .

[14] "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains." April 2018. Accessed August 2018. https://arxiv.org/pdf/1801.10228.pdf .

[15] Rilee, Kynan. "Understanding Hyperledger Fabric - Endorsing Transactions." Medium. February 09, 2018. Accessed August 2018. https://medium.com/kokster/hyperledger-fabric-endorsing-transactions-3c1b7251a709 .

[16] "What Is Digital Certificate? - Definition from WhatIs.com." SearchSecurity. Accessed September 2018. https://searchsecurity.techtarget.com/definition/digital-certificate.

[17] "Two-factor Authentication." IBM Watson. Accessed September 2018. https://console.bluemix.net/docs/services/blockchain/reference/v10_fabric.html#hyperledger-fabric.

[18] "Configuring MSP(Membership Service Provider) in Hyperledger Fabric." BlogSaays. May 11, 2018. Accessed September 2018. https://www.blogsaays.com/configure-msp-hyperledger-fabric-blockchain/ .

[19] Davies, Aran. "Pros and Cons of Hyperledger Fabric for Blockchain Networks." DevTeam.Space. August 2018. Accessed September 2018. https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-blockchain-networks/ .

[20] Cryptocurrencies Market Capitalization. Accessed September 2018. coinmarketcap.com..

Lazar Lukić, Fakultet organizacionih nauka
Kontakt: lukic.lazar95@gmail.com
Oblasti interesovanja: blockchain, kriptografija, distribuirani sistemi

Ivana Jovičić, Fakultet organizacionih nauka
Kontakt: jovicic.ivana7@gmail.com
Oblasti interesovanja: blockchain, pametni ugovori, distribuirani sistemi