Uspostava sustava za E-trgovinu

Nikolov, Giorgio

SVEUČILIŠTE JURJA DOBRILE U PULI

FAKULTET EKONOMIJE I TURIZMA „DR. MIJO MIRKOVIĆ“

GIORGIO NIKOLOV

USPOSTAVA SUSTAVA ELEKTRONIČKE TRGOVINE

Završni rad

Pula, Srpanj 2022.

SVEUČILIŠTE JURJA DOBRILE U PULI

FAKULTET EKONOMIJE I TURIZMA „DR. MIJO MIRKOVIĆ“

GIORGIO NIKOLOV

USPOSTAVA SUSAVA ELEKTRONIČKE TRGOVINE

Završni rad

JMBAG: 0145031728

Studijski smjer: Poslovna informatika

Predmet: Digitalno poslovanje

Znanstveno područje: Društvene znanosti

Znanstveno polje: Ekonomija

Znanstvena grana: Poslovna Informatika

Mentor: prof. dr. sc. Vanja Bevanda

Pula, Srpanj 2022.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____

_____

__ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

SADRŽAJ

UVOD 1

1.**ELEKTRONIČKA TRGOVINA** 2

1.2.ELEKTRONIČKA TRGOVINA U LANCU OPSKRBE 3

1.3.PREDNOSTI I NEDOSTACI ELEKTRONIČKE TRGOVINE 5

2.**BLOCKCHAIN TEHNOLOGIJA** 6

2.1.STRUKTURA PODATAKA 7

2.2.HASH FUNKCIJA 9

2.3.MERKLEOVO STABLO 9

2.4.DIGITALNI POTPIS 11

2.5.VRSTE BLOCKCHAINA 12

2.6.KONSENZUS PROTOKOLI 13

2.7.PAMETNI UGOVORI 15

2.8.PRIMJENA I PREDNOSTI PRIVATNOG BLOCKCHAINA 16

3.**HYPERLEDGER PROGRAMSKI OKVIR** 18

3.1.HYPERLEDGER FABRIC 18

3.1.1.KOMPONENTE FABRIC MREŽE 19

3.1.2.KANALI 20

3.1.3.POHRANA PODATAKA 20

3.1.4.CHAINCODE 22

3.1.5.KONSENZUS 23

3.1.6.IDENTITET ČLANOVA 24

3.2.TRANSAKCIJSKI PROCES 24

3.3.HYPERLEDGER FABRIC U LANCU OPSKRBE 28
3.3.1.UPRAVLJANJE OPSKRBOM LIJEKOVA.....30
3.3.2.PLAN TIJEK LIJEKOVA U LANCU OPSKRBE 32
3.4.OSTALE USPJEŠNE PRIMJENE.....35
ZAKLJUČAK.....37
LITERATURA.....38
POPIS SLIKA.....42
POPIS TABLICA.....42

SAŽETAK

Cilj ovog rada bio je prikazati kako se Blockchain tehnologija može iskoristiti unutar elektroničke trgovine kod lanca opskrbe. Kroz ovaj rad prikazani su ključni procesi i sudionici u B2B poslovnom modelu elektroničke trgovine kako bi dobili uvid na njenu kompleksnost i potrebu za stvaranjem efikasnijeg i sigurnijeg rješenja. Detaljno su prikazani svi elementi Blockchain tehnologije kako bi shvatili sve pogodnosti koje može imati u odnosu na klasične centralizirane sustave nabave unutar lanca opskrbe. Kombinacijom postojećih tehnologija kao što su funkcija hashiranja i digitalni potpis, peer-to-peer mreža, prikazano je kako je moguće okončati problematiku sigurnosti i transparentnosti. Prikazali smo kako u konkretnom slučaju elektroničke trgovine nije dovoljna klasična Blockchain platforma, već je bilo potrebno razviti modularna i fleksibilnija rješenja. Kroz primjer Hyperledger Fabric platforme kao primjer takve modularne Blockchain varijante, opisali smo njegove komponente, način rada i doprinos u lancu opskrbe.

KLJUČNE RIJEČI: elektronička trgovina, lanac opskrbe, Blockchain tehnologija, Hyperledger Fabric

ABSTRACT

The purpose of this paper was to demonstrate how can Blockchain technology be involved in e-commerce in the supply chain. Through this paper we have reviewed key participants and processes the B2B business model to demonstrate its complexity and the need to develop a more efficient and secure solution. All Blockchain components and concepts have been displayed in details to understand the way it can improve the current classical centralized systems. The combination of the already existing, legacy technology's like hashing, digital signatures, peer-to-peer networks, shows how it is possible to resolve issues like security and transparency. We showed on why a more modular and flexible variant is needed. Hyperledger Fabric was used as an example of such a modular architecture by explaining its components and processes.

KEY WORDS: e-commerce, supply chain, e-procurement, Blockchain technology, Hyperledger Fabric

UVOD

Svjedoci smo kako elektroničko poslovanje snažno obilježava suvremeno doba, a što je posljedica dinamičnog napretka i razvoja računarstva, informatizacije i digitalizacije tijekom proteklih nekoliko desetljeća. U skladu s time, mijenjaju se koncepcije poslovanja, poslovne suradnje i strategije, te općenito međunarodni poslovni svijet.
Zahvaljujući elektroničkom poslovanju, koje se javlja u nekoliko različitih oblika i vrsta, današnje međunarodno poslovanje susreće se s nizom prednosti ali i potrebom za stalnim napretkom. Jedan od ovih poslovnih oblika ili podsustava je i elektronička trgovina.

Cilj rada je istražiti osnovne pojmove u svezi elektroničke trgovine, analizirati značenje, razvoj, koristi i ostale odrednice navedenoga. Svrha je detaljnije istražiti B2B koncepciju poslovanja unutar lanca opskrbe, opisati njenu kompleksnost, mane i detaljno predstaviti Blockchain tehnologiju kao idealno rješenje za veliki broj prepreka s kojima se susrećemo unutar lanca opskrbe.

Rad ima tri poglavlja, uvod i zaključak. Prvo poglavlje daje širi uvod u problematiku rada. Ono obrađuje temeljne pojmove i obilježja elektroničke trgovine s naglaskom na B2B koncept poslovanja kako bi mogli shvatiti važnu ulogu koju može pridonijeti Blockchain tehnologija u lancu opskrbe. Upravo je Blockchain tehnologiji posvećeno sljedeće poglavlje u kojem se detaljno prikazuje njegov način rada i na koji način može riješiti ključne probleme unutar lanca opskrbe kao što su sigurnost podataka, transparentnost, privatnost korisnika i ukidanje svih posrednika stvarajući decentraliziranu mrežu korisnika. U trećem i posljednjem poglavlju posebna pažnja bit će usmjerena predstavljanju Hyperledger Fabric platforme kao idealno rješenje na probleme s kojima se susreću tradicionalne Blockchain mreže. Riječ je o slobodnom softveru za stvaranje privatne Blockchain mreže koji se danas često koristi kod realizacije korporativnih sustava za elektroničku nabavu.
Za potrebe istraživanja korištene su metoda analize i sinteze, induktivno-deduktivna metoda, metoda komparacije i metoda apstrakcije. Istraživanju su koristile i metoda studije slučaja, metoda kritičkog promišljanja te metoda opisivanja.

1. ELEKTRONIČKA TRGOVINA

Ponekad se u praksi elektroničko poslovanje izjednačava s elektroničkom trgovinom. Elektroničko poslovanje značajno je širi pojam elektroničke trgovine, odnosno elektronička trgovina predstavlja tek jedan od primjera, dijelova ili podsustava elektroničkog poslovanja. Optimalno je predstaviti elektroničku trgovinu kao kompleksni podsustav elektroničkog poslovanja

Elektroničko poslovanje razvilo se relativno naglo i ubrzano, a temelj njegova razvoja bio je Internet. Stoga se često govori da je elektroničko poslovanje oblik i vrsta poslovanja koji se temelji na informatičkoj tehnologiji a posebice interneta kao njegove primarne infrastrukture. Jedna u nizu definicija elektroničkog poslovanja definira ga kao transformacija klasičnog poslovanja, koja je utemeljena na integriranju poduzeća, kolaboraciji, globalnom mrežnom povezivanju i korištenju interneta kao suvremenog medija. Inicijacija njegova razvoja veže se iz 1994. i 1995. godine kada se javljaju prva web mjesta koja su potakla stvaranje koncepcije elektroničkog poslovanja (Ružić i dr., 2014).

Elektroničko je poslovanje utjecalo na povezivanje svih poslovnih subjekta diljem svijeta koji koriste računalne tehnologije i Internet, a iskazuju interes prema ovakvom obliku poslovanja. Sukladno tome, elektronička trgovina može se pojmiti kao vrsta trgovine, koja se odvija posredstvom interneta i na temelju principa elektroničkog poslovanja.

Elektronička ili e-trgovina je pojam koji označava poslovne ili komercijalne transakcije, koje, između ostaloga, uključuju prijenos podataka putem interneta. Ona obuhvaća široki raspon različitih sudionika kao što su to kupci, poslovni partneri, prodavači i njihovu međusobnu interakciju (Actualida de Commerce, 2022).
Modele elektroničke trgovine možemo podijeliti na dvije osnovne skupine:

- Trgovanje materijalnim i nematerijalnim dobrima ili uslugama;
- Trgovanje kapitalom.

Najreprezentativniji primjer elektroničke trgovine je kupnja i prodaja proizvoda i usluga. Pri tome prodavači oglašavaju svoje proizvode putem online oglasa, dok kupci iste pregledavaju u bilo koje vrijeme i na bilo kojem mjestu, uz uvjet da raspolažu uređajem

koji omogućuje Internet pretraživanje te pristup internetu. O samom razvoju elektroničke trgovine slijedi u nastavku.

1.2. ELEKTRONIČKA TRGOVINA U LANCU OPSKRBE

Strateška koordinacija poslovnih funkcija neke organizacije može biti i definicija za proces upravljanja lancem opskrbe (engl. *Supply Chain Management*). Cilj je uskladiti poslovne funkcije svih sudionika i procesa od sirovina do krajnjih kupaca. Upravljanje lancem opskrbe podrazumijeva i suradnju sa strateškim partnerima, dobavljačima i posrednicima.

Organizacija procesa upravljanja opskrbnog lanca je kompleksan proces koji zahtijeva puno posla. Kako bi se čitav proces optimizirao na najbolji mogući način, implementacija tehnoloških poboljšanja je neophodna, zbog brzine protoka informacija, velikog broja sudionika i ukupnog troška.
Implementacije IT sustava može biti rješenje administrativne složenosti sustava nabave koji se sastoji od sljedećih komponenti (Van Weele, 2014):

- Upit i naručivanje;
- Baza proizvoda, ugovora i dobavljača;
- Praćenje narudžbe;
- Dostava;
- Obrada faktura i plaćanje.

Razni informacijski sustavi razvijali su se s ciljem poboljšavanja navedenih aktivnosti. Ovdje možemo spomenuti kao platformu integrirani poslovni informacijski sustav (engl. *Enterprise Resource Planning system* – ERP). ERP podrazumijeva sveobuhvatni informacijski sustav tvrtke za upravljanje operativnim ili administrativnim procesima tvrtke, upravljanje ljudskim resursima, resursima materijala i financijskim sredstvima (Van Weele, 2014). IT sustav kojeg smatramo kao podrška u procesu nabave je sustav e-nabave (engl. *e-procurement*).
Automatizacija procesa nabave započela je još 70-ih godina s razvojem standardiziranog sustava elektroničke razmjene podataka (engl. *Electronic data interchange* – EDI). EDI omogućuje slanje standardiziranih dokumenata kao što su narudžbenice, fakture, datum isporuke, podaci o ugovoru između dva ili više računala. Takav je sustav poprilično skup, zahtijeva dedicirani hardware, software, te dodatnu

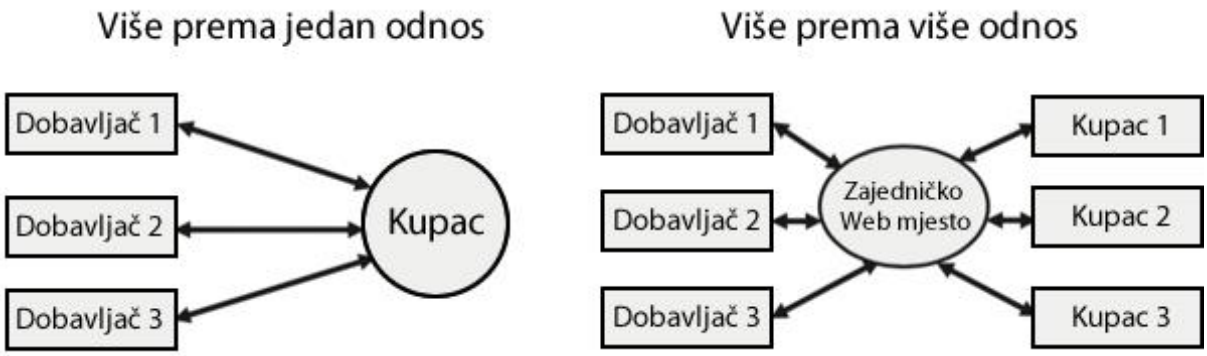
izobrazbu za korištenje (Radovilsky, 2015).

Početkom 90-ih godina, razvoj interneta doveo je i do razvoja raznih platformi za e-nabavu.

Elektronička trgovina bazirana na principu e-nabave predstavlja zbirku aktivnosti koje se odnose na proces nabave preko interneta. Ona omogućuje automatizaciju raznih aktivnosti kupnje i nabave. Kroz implementaciju platforme e-nabave svaka tvrtka očekuje smanjivanje ukupnih troškova poslovanja, povećanje prihoda, održavanje bolje kontrole resursa, te brži i efikasniji proces narudžbe (Radovilsky, 2015).

Sustav e-nabave ovisno o postojećim odnosima može biti namijenjen jednoj tvrtki koja je osnovala jedno Web sjedište prema više dobavljača u korist pregovora i nabave resursa (engl. *Many-to-one*). Više tvrtka može osnovati zajedničko Web mjesto razmjene prema više dobavljača (engl. *Many-to-many*). Takvo mjesto razmjene ne predstavlja konkurentnost nabave između osnivača, već podupire njihovu suradnju u postizanju najboljeg mogućeg ishoda nabave (Radovilsky, 2015).

Slika 1. Odnosi u elektroničkoj trgovini



Izvor: Izrađeno prema Radovilsky, Z., (2015) Business Models for E-Commerce, California State Univerity, East Bay, Str. 46.

E-nabava podrazumijeva različita rješenja kada razmatramo process nabave koje podržava (Radovilsky, 2015):

- Elektroničke tržnice – razmjena između više strana;
- Elektroničke aukcije – najpopularnije metoda kod kupaca;
- Elektronički katalozi – nabava na temelju digitalnog kataloga.

Kod elektroničke aukcije razlikujemo dvije vrste. Obrnutu aukciju (engl. *Electronic reverse auction* – e-RA), ili aukciju gdje kupac određuje cijenu nabave i najniža ponuda pobjeđuje aukciju. Druga je vrsta aukcije Aukciju unaprijed, gdje dobavljač objavljuje cijenu, a kupci zatim biraju ponudu.
Važno je napomenuti da se odvijaju u realnom vremenu i da ih obilježavaju aktualne informacije.

1.3. PREDNOSTI I NEDOSTACI ELEKTRONIČKE TRGOVINE

Danas elektronička trgovina doprinosi napretku nabave ili nabavne funkcije. Kao nova tehnologija koja unaprjeđuje sve aspekte vođenja nabave s ciljem prihoda za poduzeće i stvaranje proizvoda više kvalitete za kupca, možemo zaključiti da sustav e-nabave znatno utječe na digitalnu transformaciju svih njegovih sudionika (Spremić, 2017).

Uloga elektroničke trgovine u lancu opskrbe očituje se upravo u digitalizaciji ove funkcije, kao i strategiji reduciranja potencijalnih rizika. Među brojnim prednostima elektroničke trgovine navodi se i doprinos u internacionalizaciji nabave, boljoj dostupnosti dobavljača i inputa, kao i smanjenju zaliha i otpada u skladištima i procesu opskrbe, posredstvom digitalnog upravljanja, lakšem nadzoru i smanjenju troškova skladištenja. Svojim funkcijama elektronička trgovina omogućuje brži i veću dostupnost relevantnim informacijama, bolje povezivanje s dobavljačima, pojednostavljenje svih procesa, kao i unapređenje učinkovitosti.
Lanac opskrbe se danas može proširiti na razne procese kroz različite lokacije na globalnoj skali. To znači da imamo veliki broj sudionika, dokumenta i računa. Ako uzmemo u obzir svaki čimbenik nabave zasebno, primjećujemo da tu ima i mnogo nedostataka i prostora za napredak. Neki od osnovnih problema su transparentnost, uklanjanje posrednika, decentralizacija, povjerenje, sigurnost, smanjenje troškova i brzina transakcije. Jedna od aktualnih platformi koje mogu izići u susret svim tim problemima je Blockchain tehnologija. Dok većina poznavatelja Blockchaina veže tu platformu samo kao platforma za plaćanje, ona ima puno širi opseg primjene, i jedna od njih je baš kao platforma razmjene informacija u procesu e-nabave (Radosevic, R. 2018). Više o arhitekturi i primjeni Blockchain tehnologiji i elektroničkoj trgovini i e-nabavi slijedi u nastavku.

2. BLOCKCHAIN TEHNOLOGIJA

U ovome se poglavlju zadire detaljnije u središnju problematiku i predmet istraživanja. Definira se blockchain tehnologija te se objašnjavaju njezine vrste i specifičnosti. Posebna pažnja posvećena je funkcioniranju ove tehnologije koja u današnjici svakodnevno i vrlo intenzivno mijenja čitavi svijet.

Generalni pojam Blockchain tehnologije može se prevesti kao „Lanac blokova“. Predstavlja model pohrane podataka u podatkovnim blokovima koji su međusobno povezani i formiraju decentraliziranu, distribuiranu i javnu digitalna knjigu (engl. Ledger) (Zand i dr., 2021).

Ova distribuirana baza podataka (engl. Distributed ledger technology – DLT) autonomno se upravlja zahvaljujući peer-to-peer mreži čvorova. Svaki čvor predstavlja računalo u distribuiranoj mreži sudionika koji dijele dio svojih resursa i sudjeluje u procesiranju podataka koji se u konačnici zapisuju u blokove. Svaki čvor održava na sebi vjernu kopiju ove neizmjenjive digitalne knjige, što predstavlja dodatni sigurnosni faktor u očuvanju legitimnosti podataka na čitavoj mreži (Carnet, 2009).

Kod distribuirane baze podataka rekli smo da su zapisi pohranjeni nezavisno na svaki čvor u mreži i nema potrebe da se svaki zapis evidentira kroz neki centralni zajednički autoritativni čvor. Transakcije između čvorova su najčešće izvršene nakon postizanja nekog zajedničkog konsenzusa ili dogovora između samih sudionika, nakon čega se ažurira stanje podataka na svim čvorovima. Blockchain je specifični oblik distribuirane baze podataka jer osim što su podaci decentralizirani i njihova se vrijedna replika održava na svim čvorovima, uvodi kriptografiju kao vezu između samih blokova digitalne knjige (Saraswat, 2018).

Blockchain se temelji na kriptografiji, a evidentirani zapis se ne može mijenjati retroaktivno bez izmjene svih prethodnih blokova i bez konsenzusa mreže, svaki blok je povezan sa svojim prethodnikom (Lisk, 2018). Upravo se na tom principu temelji sigurnost ove tehnologije, što korisnicima osigurava sigurnu pohranu, provjeru i reviziju svih transakcija.

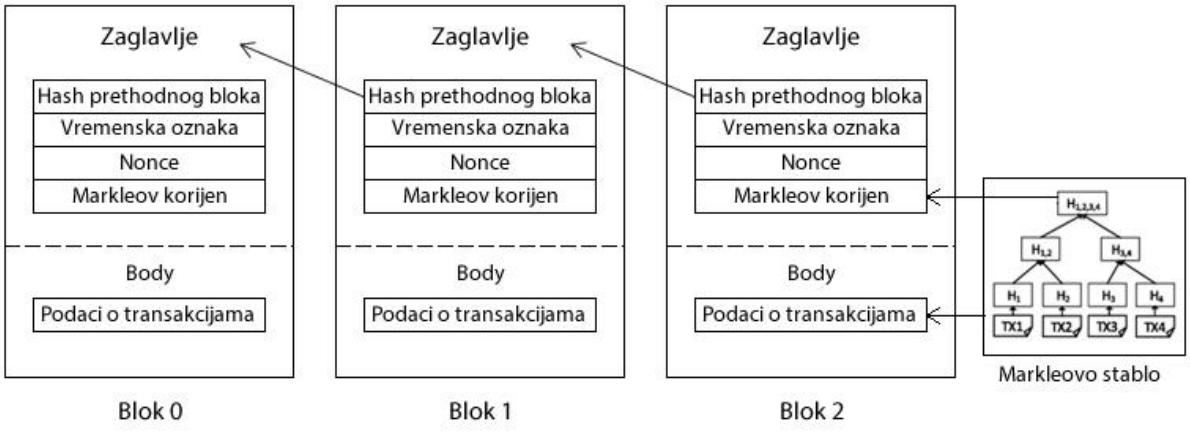
Kriptografija je u Blockchain arhitekturi potrebna radi enkripcije, hashiranja (engl. Hashing), autorizacije i autentikacije identiteta korisnika kroz digitalne potpise angažmanom privatnih i javnih ključeva. Detaljniji prikaz primjene i važnost funkcije hashiranja prikazana je u nastavku rada.

2.1. STRUKTURA PODATAKA

Temeljni sastavni dio svakog Blockchain lanca su blokovi. Svi blokovi imaju ograničenu količinu podataka koju mogu pohraniti dok nije potrebno kreirati novi.
Blok je struktura podataka koja se sastoji od zaglavlja (engl. Header) i dijela koji sadrži listu informacija (engl. Body). Jedino prvi blok (engl. Genesis block) sadrži dodatne informacije o sudionicima mreže i ostala pisana pravila.
Zaglavlje pohranjuje tehničke informacije o bloku i one su potrebne za povezivanje s ostalim blokovima u mreži:

- Vremenska oznaka – sadrži vremensku oznaku koja označava trenutak nastanka bloka;
- Hash pokazivač (engl. Hash-pointer) na prethodni blok;
- Nonce – numerička vrijednost kreirana tijekom kreiranja bloka;
- Merkleov korijen – konačna hash vrijednost Merkleovog stabla koji se nalazi u body-u bloka.

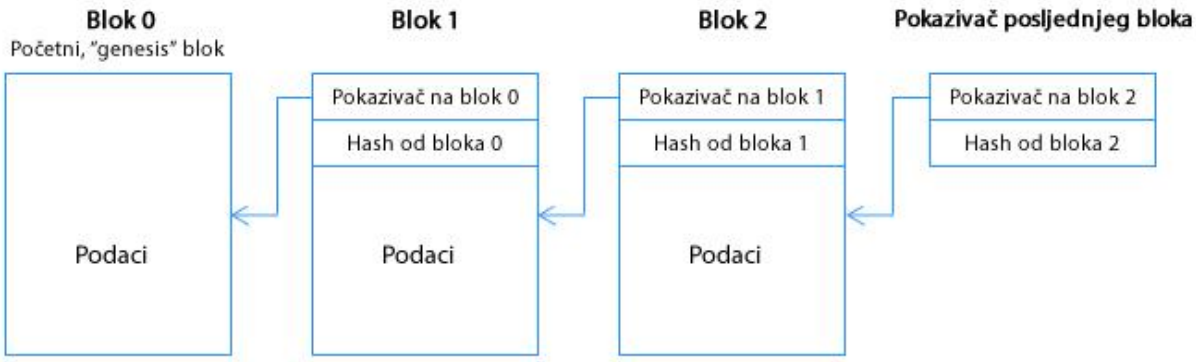
Slika 2. Prikaz strukture podataka unutar blokova



Izvor: Izrađeno prema Liang, Y. (2020.) Blockchain for Dynamic Spectrum Management. Dostupno na: https://www.researchgate.net/figure/The-structure-of-a-Blockchain-A-block-is-composed-of-a-header-and-a-body-where-a-header_fig1_337306138 *(01.06.2022.).*

Svaki zapis koji se upisuje u nepromjenjivu digitalnu knjigu prati vremenski redoslijed događaja i kriptografski je vezan za svoj prethodni blok, stvarajući tako nanizani ili povezani lanac blokova.
Novi se blokovi mogu stalno dodavati, dok se oni stari ne mogu brisati ili naknadno mijenjati.
Neizmjenjivi lanac blokova je kreiran tako što svaki blok u zaglavlju sadrži pokazivač (engl. Pointer) na prethodni blok i hash vrijednost prethodnog bloka (FER, 2017).

Slika 3. Prikaz vezanja i stvaranja neizmjenjivog lanca blokova



Izvor: Izrađeno prema Zhao, H. (2018.) Hash Pointers and Data Structures. Dostupno na: https://zhaohuabing.medium.com/hash-pointers-and-data-structures-f85d5fe91659 *(01.06.2022.).*

Potrebno je naglasiti da je Hash-pointer zapravo generiran od sveukupnog sadržaja tog prethodnog bloka, uključujući i Hash-pointer koji je taj prethodni blok imao na svog prethodnika. Kada bi netko probao izmijeniti sadržaj nekog bloka, njegova bi se hash vrijednost izmijenila, što bi automatski dovelo do toga da se hash izmijenjenog bloka i hash-pointer pohranjen u novijem bloku ne podudaraju (Zhao, 2018). U tom slučaju, blokovi koji slijede korumpiranom bloku smatrali bi se nevažećim. Napadač mreže bi tako trebao ispraviti hash vrijednosti svih blokova u lancu, i ponoviti isto na svim kopijama lanca u distribuiranoj mreži, što je gotovo pa nemoguće s obzirom na potrebnom vremenu i procesorskoj moći.

2.2. HASH FUNKCIJA

Jedan od temeljnih koncepta što čini Blockchain revolucionarnim i jedinstvenim je korištenje hash funkcije, zbog čega je bitno detaljnije shvatiti njegovu ulogu I funkciju. Blockchain tehnologija koristi hash funkciju SHA-256 kao matematičku funkciju koja pretvara bilo koji digitalni input bilo koje veličine u fiksni output, 256 bitni, koji se sastoji od 64 znamenki nazvan hash (Frankenfield, 2022).

Stvaranje hasha moguće je samo u jednom pravcu, što znači da iz generiranog hash ključa nije moguće obrnutim procesom otkriti input hash funkcije. Različiti inputi neće nikad generirati identičan hash zbog čega se hash koristi kao adresa za jednak sadržaj u peer-to-peer mreži, identifikaciju bloka i zaštitu njegovog sadržaja. Hash funkcija se zato smatra deterministočkom, jer isti input će uvijek vratiti isti rezultat (Frankenfield, 2022).

Prednosti hash funkcije su da se kroz malu količinu podataka na elegantan način može dati uvid na stanje veče količine podataka

2.3. MERKLEOVO STABLO

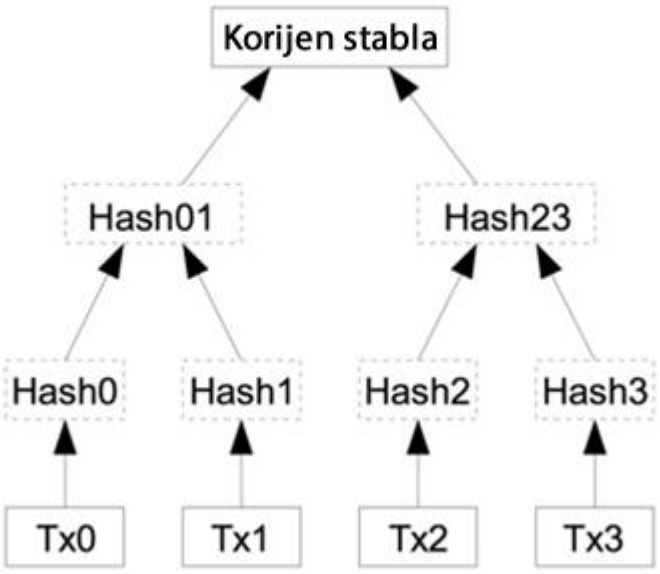
Kada smo analizirali sadržaj zaglavlja bloka, jedna od temeljnih sastavnica bio je i Merkleov korijen.

Merkleovo stablo nalazi se u body-u bloka, dok se vrijednost korijena nalazi u zaglavlju.

Merleov korijen je naziv koji se dodjeljuje konačnom hashu koji je nastao hashiranjem posljednjeg hash para u stablu, stvarajući tako digitalni otisak sadržaja stabla. Čvor Merkleovog stabla sadrži samo hash vrijednosti koje proizlaze iz prethodnih hash parova i izvornih podataka transakcija, čime se znatno smanjuje potreban prostor za pohranu podataka i učinkovitu i bržu provjeru valjanosti podataka.

Merkleovo stablo ima oblik zaokrenutog stabla. Izgradnja kreće hashiranjem listova koji se nalaze na dnu i sadrže informacije o transakcijama. Nastali čvorovi se u parovima hashiranju prema vrhu ili korijenu stabla koji sadrži konačnu hash vrijednost čitavog stabla. U slučaju da imamo neparan broj transakcija, ili listova, posljednji hash bit će dupliciran kako bi se ostvario paran broj listova (Tutorialandexample, 2022). Prikaz slijedi u nastavku (Slika 4.).

Slika 4. Prikaz Merkleovog stabl



Izvor: Wang, X. (2019.) Survey on Blockchain for Internet of Things. Dostupno na: https://www.researchgate.net/figure/Transactions-are-hashed-in-a-Merkle-Tree68_fig2_330351295 *(02.06.2022.).*

Na danom prikazu evidentna je izgradnja hash stabla uz uvjet da su u bloku zapisane četiri transakcije (Tx0, Tx1, Tx2, Tx3). Čvorovi Hash0,1,2,3 kreirani su hashiranjem pojedinačnih listova. Oni se nastavno hashiranju u parovima njihovom kombinacijom, što dovodi do nastanka čvorova Hash01 i Hash02 pa sve do korijena stabla (engl. Root Hash).

Prednost ovog rješenja je svakako u brzini i efikasnosti provjere autentičnosti podataka, zato što je dovoljno usporediti vrijednost Merkleovog korijena kako bi se utvrdila autentičnost sadržaja čitavog stabla.

Također, za provjeru autentičnosti, nije potrebno provjeravati sva stabla u mreži i svaki čvor za pronalazak neispravnosti, već se čvorovi parcijalno provjeravaju. Dovoljno rekreirati samo granu (engl. Branch) stabla u kojemu se nalazi transakcija, što drastično smanjuje broj čvorova koje je potrebno provjeriti (Mancini, 2020).

2.4. DIGITALNI POTPIS

U distribuiranim mrežama jedna od najbitnijih aktivnosti je taj da se osigura povjerenje između sudionika u sustavu. Jedna od glavnih uloga digitalnog potpisa u Blockchain mreži je autentikacija korisnika i transakcija.

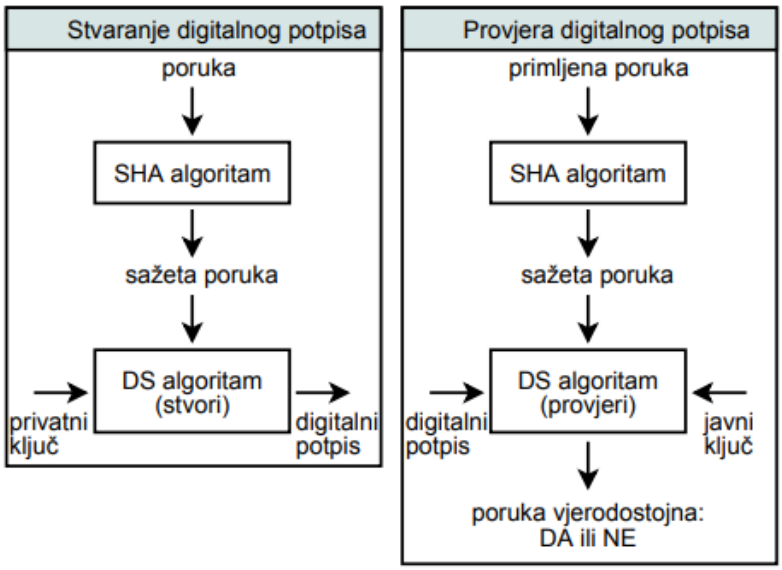
Digitalni potpis služi kao autentikacija korisnika, dokazivanjem njegovog identiteta cijeloj Blockchain mreži i u konačnici autorizira provođenje transakcije. Pod transakcijama podrazumijevamo bilo koju izmjenu podataka ili proces plaćanja koji bude uvijek u konačnici posloženi redom, sadrži vremensku oznaku i ne može biti izmijenjene (Zand i dr., 2021).

Blockchain koristi enkripciju s javnim ključem kao sigurnosni protokol za stvaranje digitalnih potpisa.

U procesu stvaranja digitalnog potpisa generira se par ključeva, privatni i javni. Javni su ključevi dostupni svima i služe za provjeru potpisa, dok su privatni ključevi dostupni samo vlasnicima što onemogućuje krivotvorenje potpisa.

Postupak stvaranja digitalnog potpisa započinje stvaranjem skraćene inačice poruke (engl. Message disgest) koristeći već prethodno spomenutu hash funkciju. Iz novonastale hashiranjem vrijednosti kroz algoritam za stvaranje digitalnog potpisa uz pomoć privatnog ključa stvara se digitalni potpis. Poruku šaljemo zajedno sa digitalnim potpisom koji se od strane primaoca provjerava putem javnog ključa. U nastavku slijedi shematski prikaz nastanka i provjere digitalnog potpisa:

Slika 5. Shematski prikaz postupka stvaranja i provjere digitalnog potpisa



Izvor: CARNET. (2007.) Digitalni potpis. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf (02.06.2022.).

Algoritmi za stvaranje digitalnog potpisa se sastoje od stvaranja javnog i privatnog ključa, stvaranja digitalnog potpisa na temelju sažete poruke I privatnog ključa te uz pomoć javnog ključa provjeriti vjerodostojnost potpisane poruke (Carnet, 2007). Najpoznatiji algoritmi za generiranje digitalnih potpisa su Digital Signature Algorithm (DSA/DSS) i Eliptic Curve Digital Signature Algorithm (ECDSA).
Digitalni potpis osim što služi kao metoda autentikacije, može biti pokazatelj integriteta primljene poruke i dokaz da se slanje poruke zaista desilo od strane autora.

2.5. VRSTE BLOCKCHAINA

Sve se vrste Blockchaina mogu uvrstiti u dvije skupine, mreže bez dopuštenja pristupa (engl. Permissionless) i s dopuštenjem (engl. Permissioned). Mreže bez dopuštenja pristupa omogućuju svakom sudioniku da anonimno postane dio mreže i svi imaju jednaka prava. U mreže s dopuštenjem pristupa može se ograničiti tko će biti dopušteni čvorovi u mreži, oni nisu anonimni i mogu im se ograničiti uloge (Wegrzyn, 2021). Može

se reći da su mreže s dopuštenjem pristupa sigurnije jer svi sudjeluju u autentikaciji transakcija, dok su mreže koje zahtijevaju dopuštenje manje sigurne ali efikasnije jer zahtijevaju manje sudionika u validaciji transakcija.

Prema strukturi razlikujemo javne, private, konzorcijske i hibridne Blockchain mreže.

Javni Blockchain karakterizira odsutnost ograničenja pristupa (engl. Permissionless). To znači da svatko tko ima internetsku vezu može postati ovjeritelj prilikom slanja transakcije ovu vrstu blockchaina. Time on sudjeluje u izvršenju konsenzusnog protokola. Ove mreže koriste neki od algoritama poput sustava dokaza o udjelu (PoS) ili sustav dokaza o radu (PoW). Kao primjer poznatih javnih Blockchaina možemo spomenuti Ethereum i Bitcoin (Privredni, 2021).

Privatni Blockchain karakterizira ograničenje pristupa, to jest moguće je pristupiti samo ako to odobre mrežni administrator. Ta jedna središnja vlast osim što odlučuje o sudionicima, određuje I njihova prava. Može se reći da je privatni Blockchain parcijalno decentraliziran jer je pristup na mrežu ograničen (Wegrzyn, 2021).

Konzorcijski Blockchain je mreža koja zahtjeva dopuštenje pristupa. Taj model upravlja više organizacija koje sudjeluju u mreži, za razliku od privatne mreže di imamo jednu centraliziranu vlast.

Iz toga proizlazi da je konzorcij više decentraliziran i sigurniji od private mreže ali zato predstavlja puno veći napor za uspostavu jer se ista standardizacija treba provesti kroz sve organizacije koje su sudionici mreže (Wegrzyn, 2021).

Hibridni Blockckchain je kombinacija javnog i privatno/konzorcijskog modela, gdje mrežu vodi i kontrolira jedna središnja organizacija uz nadzor javnog Blockchaina koji je potreban za autorizaciju I autentikaciju određenih transakcija (Wegrzyn, 2021).

2.6. KONSENZUS PROTOKOLI

Povjerenje je jedan od ključnih odrednica funkcioniranja na kojem se temelji Blockchain. Pošto se radi o decentraliziranoj mreži, ne postoji neka centralna vlast koja će provjeravati i uvažavati transakcije. Bez obzira na to, sigurnost i valjanost transakcija omogućuju razni konsenzus protokoli (Zand i dr., 2021).

Konsenzus protokoli omogućuju da se čvorovi u mreži mogu međusobno dogovoriti o konačnom slijedu blokova. Svaki čvor sadrži kopiju digitalne knjige i može provjeriti transakcije u novom bloku i time potvrditi ispravnost novog bloka (Cardanians, 2019). Na taj način konsenzus protokol osigurava da je novo dodani blok autentičan. Za

njegov nastanak potrebna je suglasnost većine čvorova u mreži. Svaki protokol definira pravila koja se moraju slijediti za postizanje sporazuma, i nastoji udovoljiti neki zajednički ishod koji odgovara svim čvorovima. U tom zbiru pravila definiraju se i čvorovi koji su odgovorni za kreiranje bloka, dok će ostali čvorovi provjeravati njegovu autentičnost.

Proof of Work (PoW) je najzastupljeniji oblik konsenzusa korišten na Blockchain platformama kao što su Bitcoin i Ethereum. Ovaj se konsenzus zasniva na rješavanju kompleksnih matematičkih hash izračuna.
Svi čvorovi sudjeluju u procesu izračuna, rudarenju (engl. Mining), i mogu se udružiti u veće skupine (engl. Pools) kako bi ujedinili računalnu snagu i imali veće izglede za pronalazak točnog rješenja. Novi blok kreirat će čvor koji prvi riješi matematički problem te isti će biti i nagrađen. U zaglavlju bloka unutar nonce variable zapisuju se koraci koji su bili potrebni za izračun kao dokaz za ostale čvorove u mreži. Smatra se da ova metoda nije energetski učinkovita jer izračun tih kompleksnih matematičkih zadataka zahtijeva veliku količinu računalne snage ili potrošnju električne energije (Zand i dr., 2021). Osim velike potrošnje energije, kreiranjem velikih udruženja rudara umanjuje se sveukupna decentralizacija sustava.
Proof of Stake (PoS) je oblik konsenzusa koji nasumice bira kreatora i validatora novog bloka. Vjerojatnost da će se neki čvor biti odabran ovisi i o njegov ulogu (engl. Stage). Proces stvaranja novih blokova u ovom se procesu zove minting. Kao zaštitni mehanizam, u slučaju da se dozvole lažne transakcije, načinjena šteta se oduzima iz uloga čvora koji je bio zadužen za mintanje (Mycointainer, 2020). Ovaj sustav nema problema s decentralizacijom troši puno manje energije i mnogo je brži.

Proof of Authority (PoA) je zapravo modificirana verzija PoS gdje validatori transakcija mogu biti samo odabrani članovi. U takvoj mreži svi su članovi poznati i pogodno su rješenje kod sustave e-nabave (Tahereh Nodehi i dr, 2020).

2.7. PAMETNI UGOVORI

U distribuiranoj mrežnoj arhitekturi kao što je Blockchain koriste se decentralizirane aplikacije (engl. Decentralized applications – Dapps). Takve se vrsta aplikacija vrti na više računala istovremeno unutar mreže. U slučaju peer-to-peer mrežne arhitekture decentralizirane aplikacije dizajnirane su tako da svaka instanca programa predstavlja istovremeno server i klijenta (Frankenfield, 2021).
Decentralizirane aplikacije na Blockchain mreži sastoje se od softvera (engl. Client) koji omogućuje interakciju korisnika s ostatkom mreže, pametnih ugovora i Blockchain mreže.
Funkcioniranje decentraliziranih aplikacija omogućuju pametni ugovori (engl. Smart contracts), odnosno programski kod koji predstavlja poslovnu logiku koja se izvodi i nalazi na Blockchain mreži.
Njihov nastanak seže još davne 1997 godine kada ih je Nick Szabo definirao kao „skup obećanja, specificiranih u digitalnom obliku, uključujući protokole unutar kojih stranke izvršavaju ostala obećanja“. Automatski se pokreću i izvršavaju unaprijed zadane zadatke, stvarajući tako jednu vrstu sporazuma kako bi svi sudionici bili sigurni u njegov ishod bez potrebe sudjelovanja posrednika (IBM, pristup 18.06.2022). Funkcioniraju na principu postavljenih uvjetovanih izjava koje su upisane unutar ugovora poput formule kao što su “ako/kada (je ispunjen određen uvjet)“ te “onda (se radnja izvršava)“.
Pametni ugovori nemaju mnogo funkcija prema Blockchain mreži. Oni mogu upisivati nove podatke u blokove ili čitati već postojeće podatke, zato se mogu najbolje iskoristiti tako da očitaju trenutne upisane podatke iz nekog bloka, iz njihovih vrijednosti pokrenu neku poslovnu logiku i za kraj ažuriraju blok novim nastalim podacima (Zand i dr., 2021).
Danas je najpoznatija decentralizirana platforma koja se temelji na pametnim ugovorima Ethereum. Pametni ugovori se pokreću se unutar Ethereum virtualnog stroja (engl. Ethereum Virtual Machine - EVM) i programiraju se pomoću Solidity programskog jezika. Pametni ugovori se pokreću u vlastitoj okolini, izolirana od ostatka mreže unutar vlastitog virtualnog stroja (engl. Virtual machine – VM) i Docker kontejnera kako bi ograničili utjecaj mogućih bagova na ostale komponente mreže (Moralis, pristup 18.06.2022).

Svaki je čvor u ovoj mreži odgovoran za održavanje ispravnog rada mreže i izvođenje pametnih ugovora .

Pametne ugovori mogu biti korisni za razne vrste poslova koji se kreću od financijskih usluga, kredita, prijenosa vlasništva, pravnih postupaka pa do kompleksnih procesa automatizacije i praćenja u sustavu elektroničke nabave.

2.8. PRIMJENA I PREDNOSTI PRIVATNOG BLOCKCHAINA

Blockchain ima široku primjenu. Ova tehnologija omogućuje sudjelovanje većem broju računala i korištenje osnovnih prednosti. Danas postoje brojni primjeri njihova korištenja u praksi, kao i funkcionalnosti koje podržavaju određene industrije i sektore.

Od ostalih prednosti i argumenata primjene izdvaja se i nepovjerljivost. Naime, ova tehnologija omogućuje odvijanje digitalnih transakcija strankama koje si međusobno ne vjeruju.
Transparentnost i sigurnost postižu se distribuiranjem knjige na mnoge čvorove i njezinom sinkronizacijom putem fleksibilnih politika konsenzusa. Ova tehnologija omogućuje sudionicima, iako si ne vjeruju, da budu sigurni tako što se sve transakcije mogu detaljno pratiti. Nakon potvrde transakcije istu je gotovo nemoguće poništiti. Primjerice, kod bitcoina, Blockchain može istražiti i otkriti broj bitcoinova na bilo kojem računu, ili trag gdje su raspoređena sredstva.

Decentralizacija je sljedeća prednost. Ona se odnosi na smanjenje centraliziranih monopola i minimiziranje troškova. Blockchain mreža podržava ekonomiju razmjera, bez centraliziranog ulaganja. Time se na tržištu povećava konkurencija, smanjuju barijere, a poslovanje postaje učinkovitije (Lisk, 2022).
Skup ovih ključnih prednosti čine primjenu Blockchain tehnologije od velike koristi u raznim industrijama, pogotovo u situacijama kada je potrebna implementacija privatne mreže korisnika gdje ne postoji međusobno povjerenje (Wachal, 2021).
Doprinos financijskom sektoru očitovan je i u kontekstu standardizacije, skalabilnosti, pravne sigurnosti, interoperabilnosti i suradnje. Time se može istaknuti kako blockchain i korištene platforme na ovome primjeru mijenjaju dosadašnje financijsko poslovanje.
Financijski sektor je samo jedan od slučajeva u kojem Blockchain može biti od velike važnosti. Zdravstveni sektor pokazuje veliki potencijal zbog umreženosti velikog broja

organizacija i visoke važnosti održavanja privatnosti osobnih podataka pacijenta. Automatizacija strojeva i energetika mogu iskoristiti prednost integritet i sigurnost podataka u stvaranju pametnih gradova i interoperabilnost raznih energetskih sustava radi postizanja više efikasnosti.

U zadnjim desetljećima, elektronička nabava postala je globalna, i zahtjeva razvoj privatnih mreža sigurne, transparentne komunikacije, s potrebom smanjivanja troškova i bržim i efikasnijim sustavom sklapanja ugovora međunarodnih transakcija. Jedan od poznatijih sustava nabave koji se bazira na Blockchain tehnologiji je „IBM Food Trust“. IBM je razvio ovu platformu nabave prehrambenih namirnica u suradnji s ostalim sudionicima lanca nabave kao što su Nestle, Walmart, Dole Food company i Golden State Foods. Svi su oni vidjeli potencijal i korisnost ove platforme kao što su uvid u porijeklo namirnica, njena sigurnost, svježina, autentičnost certifikata, efektivnija komunikacija, smanjenje otpada i privatnost podataka (IBM, 2019). Za kreaciju takve privatne mreže, nije bila dovoljna samo IBM-ova Blockchain platforma, nego kao i u mnoštvo platforma za suradnju i e-nabave korištena je i Hyperledger Fabric sustav kojeg ćemo detaljnije proučiti u nastavku ovog rada.

3. HYPERLEDGER PROGRAMSKI OKVIR

Hyperledger je projekt koji se pojavio 2015. godine, od strane Linux fondacije. U suvremeno doba, zahvaljujući svojim komponentama, obilježjima i načinu funkcioniranja, podržava razne industrije i ima široku primjenu. U ovome poglavlju detaljnije se raspravlja o njegovim komponentama, sudionicima i načinu funkcioniranja.

Temeljni cilj ove platforme je promicanje međusektorske suradnje putem razvoja blokova i distribuiranih registara. Poseban naglasak postavljen je na unapređenje performansi i pouzdanosti. U današnjici ova platforma podržava globalne poslovne transakcije, velike tehnološke procese, financijske aktivnosti i lance opskrbe (IBM, 2022).

Jedna od bitnih karakteristika je mogućnost dijeljenja privatnih podataka između manjih skupina sudionika platforme, što je jako praktična primjena u velikim korporativnim i poslovnim udruženjima (Zand i dr., 2021).
Hyperledger paletu proizvoda trenutno čini tri distribuiranih registra koji se temelje na Blockchain tehnologiji, Sawtooth, Iroha i Fabric. Ostali proizvodi Hyperledger palete su također orijentirani na Blockchain tehnologiji, ali pokrivaju specifične funkcije kao što su očuvanje identiteta, interoperabilnost, pametni ugovori i slične funkcionalnosti (Ledgerinsights.com, 2019).

Ovo je poglavlje posvećeno Hyperledger Fabric programskom okviru pa u narednom dijelu slijedi detaljnije o njemu i načinu funkcioniranja.

3.1. HYPERLEDGER FABRIC

Hyperledger Fabric je platforma za izgradnju distribuirane Blockchain platforme koja zahtjeva dopuštenje pristupa, što znači da su svi sudionici u mreži djelomice poznati. Cilj je bio stvoriti fleksibilnu platformu namijenjenu poslovnim subjektima kod raznih primjena i razina sigurnosti. Može se reći da je to zapravo platforma namijenjena sudionicima koji imaju neki zajednički poslovni cilj ali nemaju međusobno potpuno povjerenje (IBM, 2018).
Jedinstven je zbog svog modularnog dizajna koji se sastoji od praktičnih funkcionalnosti kao što su to integriranim model autentikacije, autorizacije i

prilagodljiva politika odobravanja transakcija. Korisnici u transakcijama poznati i moguće je upravljati identitetima i njihovim pravima. Rezultat je povjerljiva komunikacija između svih članova mreže bez potrebe da informacije moraju prolaziti kroz neku središnju vlast.

Fabric omogućuje paralelnu i učinkovitu obradu podataka i promjenjivu poslovnu logiku koju ostvaruje pomoću pametnih ugovora koji se u Hyperledger Fabrik okruženju nazivaju chaincode (Zand i dr., 2021).

Osim modularne prednosti, Fabrik arhitektura se bitno razlikuje od ostalih mreža bez dopuštenja pristupa kao što su to Ethereum i Bitcoin gdje se transakcijski proces svodi po „Ordee-Execute“ modelu dok se kod Fabric-a transakcijski proces odvija po „Execute-Order-Validate“ modelu (Zand i dr., 2021). Detaljniji prikaz transakcijskog procesa Fabric platforme slijedi u nastavku rada.

3.1.1. KOMPONENTE FABRIC MREŽE

Kao i u drugim Blockchain mrežama, Hyperledger Fabric decentraliziranu mrežu čine članovi (engl. Peers) koji se odnose na digitalne entitete koji sudjeluju u radu čitave mreže svojim računalnim resursima. Članovi u Fabric mreži nisu svi jednaki, već imaju različite i precizno definirane uloge.
Prema ulozi, razlikujemo tri osnovne vrste članova, a to su klijenti, ravnopravni članovi (engl. Peers) i servis za redanje transakcija (engl. Ordering peers) (Softwaremill, pristup 24.06.2022).

Klijenti predstavljaju krajnje korisnike koji prozivaju transakcije. To je aplikacija koja omogućuje interakciju s Fabric mrežom. Fabric je razvio vlastiti računalski alat (engl. Software development kit – SDK) za razvoj aplikacija namijenjene klijentima i razvoj pametnih ugovora. Komunikaciju pre ravnopravnim članovima mreže i uređivačima omogućuje aplikacijsko programsko sučelje (engl. Application programming interface – API).

Posebno se razlikuju članovi koji izvršavaju transakcije i održavaju dnevnik transakcija. Ravnopravni čvorovi imaju ulogu potvrđivanja valjanosti transakcija prije samog upisivanja u dnevnik transakcija. Takvi se članovi nazivaju „Committing peers“, oni sadrže kopiju dnevnika transakcija za svaki kanal u kojem sudjeluju, provjeravaju ako je transakcija odobrena i potvrđuje valjanost rezultata. Članovi koji u sebi sadrže

pametne ugovore i prozivaju se od strane klijenta kako bi izveli funkcije pametnog ugovora i odobrili ishod simulacije nazivaju se „Endorsing peers“ (Medium.com, pristup 26.06.2022).

Odobrene transakcije se od strane klijenta šalju dalje prema servisu za redanje transakcija koji kronološki reda transakcije i formira novi blok kojeg šalje na ponovnu provjeru prema članovima za potvrđivanje prije nego što ih isti zapišu u dnevnik transakcija. Detaljni prikaz čitavog transakcijskog procesa slijedi kasnije u nastavku rada.

3.1.2. KANALI

Klijent, ravnopravni članovi i sustav za uređivanje zajedno tvore kanal (engl. Channel) u kojem dijele zajedničku digitalnu knjigu i samo članovi tog kanala imaju uvid u njen sadržaj. Svaki član može formirati sa drugim članovima zasebni kanal koji postaje nezavisna blockchain mreža sa vlastitom distribuiranom digitalnom knjigom stanja (HF Redhatdocs, pristup 24.06.2022).

Stvaranje kanala je jedan od prvih I najvažnijih koraka u stvaranju Fabric mreže jer je ona potrebna da se prošire postavke mreže na sve članove. Upravo korištenje apstrakcije kanala omogućuje povezivanje raznih organizacija koje međusobno dijele informacije ali nemaju potpunog povjerenja jedni u druge. Svaki član u kanalu sadrži kopiju svih transakcija i ima uvid u podatke koje možda ne želi podijeliti sa drugim organizacijama. Rješenje je upravo stvaranje zasebnih kanala između različitih organizacija kako bi se ograničio pristup podacima (Hejduk, 2021).

3.1.3. POHRANA PODATAKA

Član koji pripada nekom kanalu odgovoran je za čuvanje kopije distribuirane glavne knjige, tj. dnevnik transakcija (engl. Ledger) i pokretanje pametnih ugovora koji se u Fabric mreži nazivaju chaincodes.

Dnevnik transakcija na svakom je članu sastavljen od lanca blokova koje je posložio sustav za uređivanje. Svaki blok sadrži informacije o transakcijama i nepromjenjiv je. Dnevnik transakcija sadrži sve uspješne ali i neuspješne pokušaje promijene stanja.

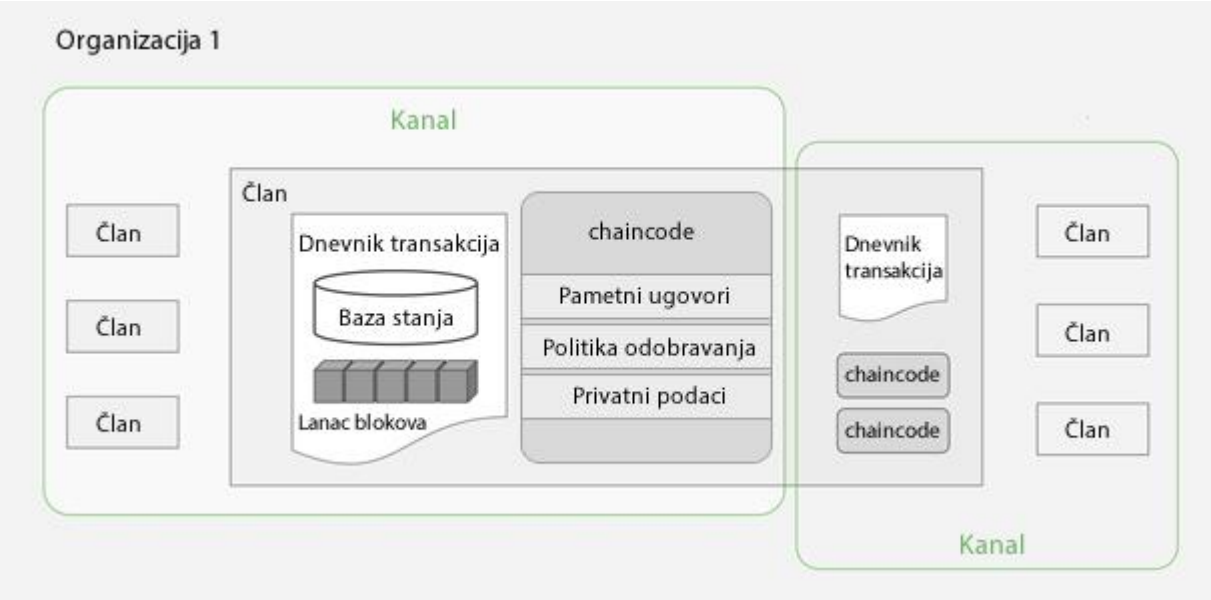
Fabric koristi još jednu dodatnu komponentu za pohranu podataka unutar članova, a to je baza podataka stanja (engl. World state) ili svjetsko stanje. Za razliku od dnevnika transakcija, baza podataka stanja je izmjenjiva. Ona sadrži aktualne vrijednosti unutar

blockchain-a. Informacije su organizirane kao kolekcija parova ključ-vrijednost (engl. Key value pair) unutar NoSQL baza podataka kao što su CouchDB ili LevelDB. Pošto prikazuju indeksiran prikaz dnevnika transakcija, koristi se s ciljem unaprjeđenja performansi rada pametnih ugovora, tako što za provjeru stanja ne moraju prolaziti kroz sve transakcije, već imaju odmah uvid u posljednje ažurirane vrijednosti

Dodatnu funkcionalnost koju nudi Fabric je stvaranje kolekcija privatnih podataka. Oni se mogu dijeliti između svih članova kanala, samo pojedinačnih članova kanala ili čak sa različitim članovima iz drugih kanala. Može biti korisna opcija u slučaju da želimo sakriti cijenu ponude od jedne skupine kupaca u korist druge skupine.

Fabric koristi važan protokol pod nazivom Fabric Gossip koji ima zadaću sinkronizirati podatke unutar baza podataka stanja kod svih članova koji nisu sudjelovali u validaciji transakcije. Osim toga, ima bitnu ulogu u otkrivanju podatak novo nastalih korisnika čitavoj mreži ili pak o statusu nekog člana koji možda više nije dostupan. Gossip protocol je također zadužen za dijeljenje čitavog relevantnog svjetskog stanja novim članovima (Rilee, 2018). Na taj način svi podaci ne trebaju uvijek prolaziti kroz servis za redanje transakcija čime se znatno povećavaju performance mreže.

Slika 6. Sastavni dijelovi za pohranu podataka unutar članova i kanala.



Izvor: Izrađeno prema Softwermill, Hyperledger Fabric Cheat Sheet. Dostupno na: https://softwaremill.com/hyperledger-fabric-cheat-sheet/ *(19.06.2022.).*

Iz prikaza sastavnih dijelova korištenih kod pohrane podataka unutar Fabric mreže (Slika 6.), vidljivo je kako jedan član može biti dio dva različita kanala unutar iste organizacije i time omogućuje uvid u dnevnik transakcija, pristup privatnoj kolekciji podataka i korištenje jednakih pametnih ugovora za oba kanala.

3.1.4. CHAINCODE

Pametni ugovori ili chaincodes u Fabric-u nisu samo pametni ugovori, već su oni u zasebni kontejneri koji u sebi sadrže politike za odobrenje transakcija i razne kolekcije privatnih podataka (Softwaremill, pristup 24.06.2022). Politika za odobrenje transakcija je usko vezana za sam ugovor jer ona definira koje organizacije moraju dozvoliti pokrenutu transakciju od strane pametnog ugovora kako bi ona bila valjana.
Provode se ako su svi uvjeti politike za odobrenje transakcija ispunjeni. Oni ne interagiraju direktno s Blockchainom već su u stalnoj interakciji sa bazom podataka stanja, gdje čitaju, brišu ili upisuju nove podatke.
Sadržavaju poslovnu logiku i instrukcije za kreiranje ili izmjenu imovine u Blockchainu. Kako bi funkcionirali, potrebno je da su instalirani unutar članova i pokreneuti u kanalu. Ostale organizacije koje žele koristiti isti pametni ugovor, moraju ga instalirati na svog člana.Unutar mreže postoje korisnici koji imaju prava za pristup ili instalaciju ugovora. Za razliku od pametnih ugovora koji se temelje na Ethereum Blockchain mreži, Fabric podržava pametne ugovore pisane u različitim jezicima kao što su GO, JavaScript ili Java. Ovi programi se izvode u Docker kontejnerima i podatke koje zapišu u njihovom svjetskom stanju, dostupni su samo tom pametnom ugovoru. Pametni ugovori u Fabric mreži mogu prozvati funkcije drugog ugovora ako im je pristup dozvoljen (Github.io, pristup 25.06.2022).

3.1.5. KONSENZUS

Opći dogovor ili suglasnost (engl. Consensus) koristi se u postizanju sporazuma oko valjanosti neke vrijednosti između više članova u distribuiranoj mreži. Pretpostavka je da će mreža članova uspješno funkcionirati u okruženju parcijalnog povjerenja.
Opći dogovor o valjanosti transakcija u Fabric mreži postiže se kroz suradnju ova tri mehanizma (Kumar, 2018):

- Politika odobravanja transakcija;
- Servis za redanja transakcija;
- Validacija.

Politike odobravanja transakcija definiraju pravila koja treba slijediti kako bi se izvođenje nekog pametnog ugovora i njegov rezultat mogli smatrati uspješnim. Pomaže oko odluke ispravnosti određene transakcije.
Logika odobravanja mora biti instalirana na članovima koji su odabrani i odgovorni za odobravanje transakcija.
Ona definira koji članovi moraju potvrditi ispravnost transakcije da bi se ona smatrala valjanom i potom zapisala u dnevnik transakcija.
Smatra se valjanom ako su u validaciji sudjelovali samo odabrani članovi organizacije, većina je suglasna, svi imaju valjane digitalne potpise i vraćaju jednaki rezultat iz provedene transakcije.

Politika odobravanja transakcija može biti krojena po mjeri i potrebama aplikacije tako da se odredi bilo koja kombinacija suglasnosti članova potrebna da odobri transakciju.

Jedna od komponenti što čini Fabric jedinstvenim je Servis za redanje transakcija (engl. Ordering service) ima ulogu slaganja transakcija po kronološkom redoslijedu i grupirati ih u blokove. Ovaj servis nije odgovoran za sadržaj transakcije već samo za njihov redoslijed upisivanja unutar bloka. Sve odobrene transakcije koje stignu do servisa za redanja poslože se unutar bloka koji se šalje na sve članove unutar kanala koji će izvršiti ponovno provjeru transakcija i upisati blok u vlastitu kopiju dnevnika transakcija.
Kako ispunjava vitalnu funkciju mreže, bitno je da bude decentraliziran, otporan na potencijalne malverzacije i da njegova uloga bude distribuirana među više pripadnika mreže. Postoje različiti algoritmi koji se mogu implementirati unutar servisa za redanje transakcija radi postizanja suglasnosti oko njihovog redoslijeda. Trenutno najpoznatiji

su Solo, Kafka i Raft. Posljednja dva omogućuju redanje transakcija kroz više decentraliziranih čvorova, na način da je čitav sustav otporan na kvarove (engl. Crash fault tolerant – CFT) i omogućuje postizanje konačnog dogovora i u slučaju da pola instanci prestane raditi zbog neke vrste kvara.
Posljednji uvjet u postizanju općeg sporazuma o valjanosti transakcije je potvrđivanje valjanosti transakcija poredanih u novo nastalom bloku.
Svi članovi vrše dodatnu validaciju ispravnosti transakcija i upisuju blok u vlastitu kopiju dnevnika transakcija. U slučaju da su transakcije neispravne, upisuje se unutar bloka kao nevažeće transakcije dok se baza podataka stanja ažurira samo u slučaju kreacije ispravnog bloka.

3.1.6. IDENTITET ČLANOVA

Za svakog sudionika unutar Fabric mreže postoji jedan digitalni identitet upisan unutar X.509 certifikata koji služi kao identifikacija za samog člana mreže (Redheaddocs.io, pristup 26.06.2022).
Digitalne identitete izdaje povjereno tijelo za izdavanje certifikata (engl. Certificate Authority – Fabric CA). Svaka organizacija ili skup članova ima vlastito tijelo za izdavanje certifikata zbog čega je potrebna još jedna komponenta koja će te digitalne identitete prepoznati i pretvoriti u legitimne članove Fabrik mreže. Ovu ulogu preuzima servis članarine (engl. Membership Service Provider – MSP) koji osim prepoznavanja i validaciju identiteta vrši još jednu bitnu ulogu, a to je definiranje koja prava i ulogu ima pojedini član unutar kanala, organizacije ili čitave mreže. Servis članarina također posjeduje javne ključeve svih članova kako bi mogao provjeriti njihove digitalne potpise (Redheaddocs.io, pristup 26.06.2022).

3.2. TRANSAKCIJSKI PROCES

Tradicionalne Blockchain platforme prate sekvencijalnu izvedbu transakcija, gdje se transakcije izvode od strane svih čvorova nakon postizanja općeg dogovora oko egzekucije (IBM, 2018). Riječ je o tako zvanom „order-execute“, tradicionalnom pristupu gdje svi članovi istovremenu sudjeluju u rudarenju kako bi kreirali blok prije nego uopće započinju sa stvaranjem redoslijeda transakcija. Jednom kada je blok stvoren, svi članovi ponovno pokreću sekvencijalno transakcije iz bloka kako bi

provjerili valjanost rezultata i tek onda definitivno zapisuju novonastali blok u dnevnik transakcija (IBM, 2018).

Slika 7. Order-execute Blockchain proces izvođenja transakcija.

Izvor: IBM, (2018) Behind the Architecture of Hyperledger Fabric. Dostupno na: https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/ (19.06.2022.).

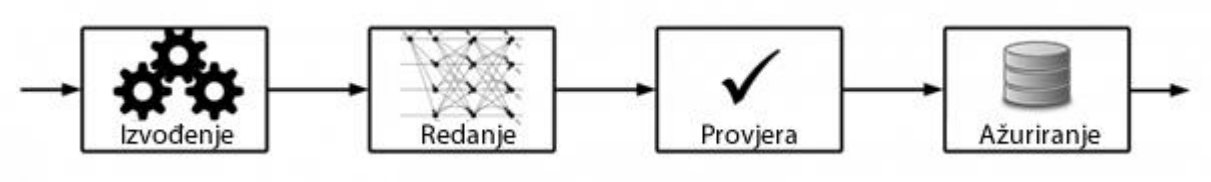
Nedostaci u ovakvoj arhitekturi su jako loše performanse zbog toga što svi članovi sudjeluju u pokretanju i validaciji transakcija. Svi članovi rade jednak posao i podaci iz transakcija vidljivi su svima, što umanjuje privatnost.
Kod „order-execute“ arhitekture, izvođenje transakcija i upisivanje podataka unutar Blockchaina objedinjuju se zajedno unutar istog pojma, transakcija. Hyperledger Fabric odvaja korake unutar transakcijskog procesa kao zasebne pojmove i ideje.

Modularna arhitektura Fabric programskog okvira raščlanjuje transakcije na tri faze i to (Sumit V, 2019):

- Simuliranje transakcije;
- Redanje transakcija u blokove;
- Potvrda i spremanje transakcije.

Ovakav koncept izvođenja transakcija nazivamo „execute-order-validate“ arhitekturom, koja omogućuje izvođenje transakcije prije nego što se dostigne opći dogovor oko redoslijeda transakcija u bloku.

Slika 8. Tijek execute-order-validate Fabric procesa izvođenja transakcija.



Izvor: IBM, (2018) Behind the Architecture of Hyperledger Fabric. Dostupno na: https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/ (19.06.2022.).

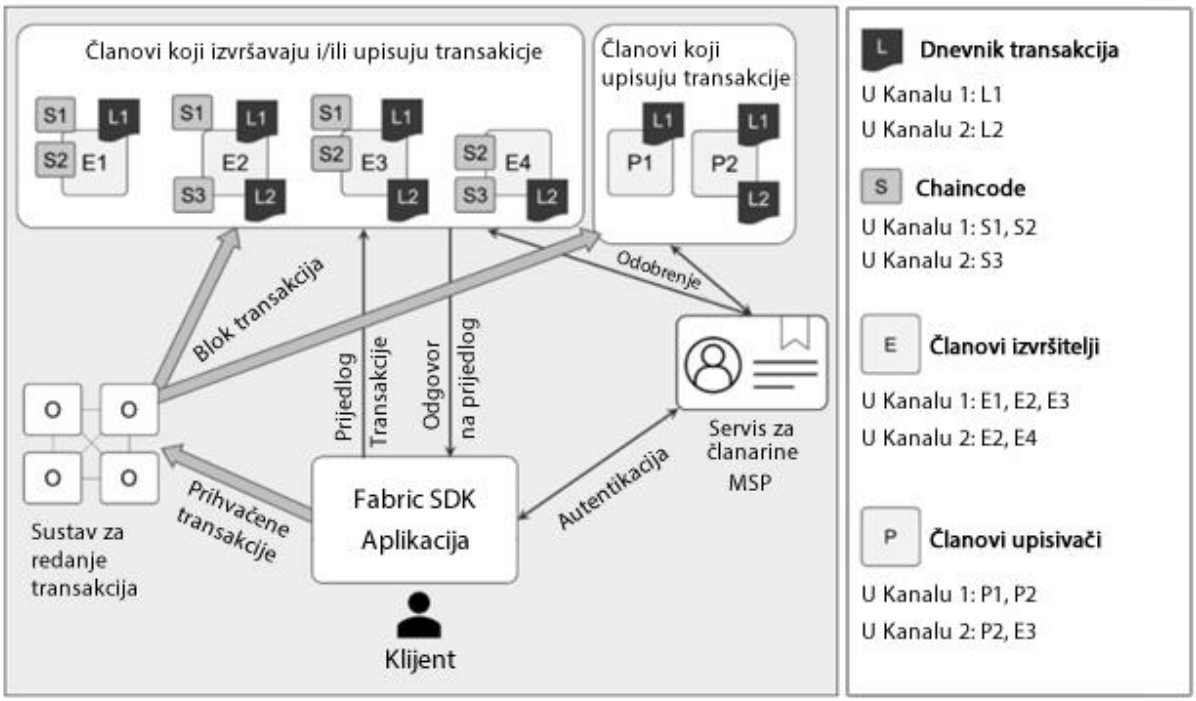
Korisnik može pristupiti klijentu nakon što je uspješno pribavio identifikaciju na mreži i pozvati određenu funkciju iz pametnog ugovora s odgovarajućim parametrima i stvara prijedlog transakcije.

Članovi koji sadrže odgovarajući pametni ugovor zaprimiti i zaduženi su za odobravanje transakcije „Endorsing peers“, zaprimit će prijedlog transakcije i provjeriti ispravnost formata prijedloga tako što će provjeriti ako je ista transakcija već provedena ili ako je potpis korisnika ispravan i posjeduje odgovarajuća prava za izvršenje transakcije na određenom kanalu. Nakon uspješne provjere, članovi izvršavaju simulaciju transakcije koristeći ulazne parametre i trenutno stanje na mreži. Simulirani prijedlog transakcije se šalje natrag aplikacijskom klijentu koji u ime korisnika prikuplja sve odobrene transakcije i provjerava ispunjenje svih uvjeta prema politici odobravanja.

Ako je su svi postavljeni uvjeti ispunjeni, transakcije se šalju iz aplikacijskog klijenta ka servisu za određivanje redoslijeda transakcija „Ordering service“ koji će kronološki poredati transakcije te ih grupirati u blokove. Novo kreirani blok se zatim šalje svim članovima na ponovnu provjeru.

Članovi koji prime novi blok od strane servisa za redanje transakcija „Committing peers“, provjeravaju još jednom ako su se transakcije provele na valjanim članovima, ako se politika odobravanja ispoštovala, da se podaci nisu izmijenili između prve i druge provjere i da nema konflikata u novo nastalim podacima s onim koji su zapisani u bazi podataka stanja. Dupla provjera sprječava i duplo izvođanje transakcija (engl. Double spending). Ako je provjera uspješno izvedena, njeno se stanje zapiše u bazi podataka stanja i evidentira u Blockchain mreži. U slučaju de je validacija neuspješna, zapisuje se u blockchain kao nevažeća transakcija.

Slika 9. Prikaz transakcijskog procesa unutar Hyperledger Fabric mreže.



Izvor: Izrađeno prema Nodehi, T., (2020) A Blockchain Based Architecture for Fulfilling the Needs of an E-Procurement Platform *Dostupno na:* http://www.ieomsociety.org/detroit2020/papers/64.pdf *(19.06.2022.).*

Čitav transakcijski proces izdvojen je u zasebne komponente koji se ne izvode na svakom članu unutar mreže, već svaki član ima točno definiranu ulogu, što omogućuje paralelno izvođenje transakcija i upisuju se u Blockchain tek nakon što je dogovoren redoslijed transakcija.
Transakcije ne moraju pratiti kronološki red izvođenja dok god nisu u nekom međusobnom vrijednosnom konfliktu. Ovakva politika izvođenja drastično utječe na performanse poboljšava brzinu transakcijskog procesa.
Možemo zaključiti da modularna arhitektura i fleksibilnost Fabric procesa omogućuju da se čitav proces transakcija kroji i izvodi po mjeri sudionika mreže uz značajno bolje performanse i razine privatnosti u odnosu na tradicionalne „order-execute“ modele.

3.3. HYPERLEDGER FABRIC U LANCU OPSKRBE

Tradicionalnom lancu opskrbe najčešće nedostaje transparentnosti i manjak pouzdanosti u kreiranim izvještajima. Veće tvrtke imaju privatne sustave za vođenje podataka na koje manje organizacije koje sudjeluju u procesu nabave nemaju pristupa ili je tehnički i cjenovno pre zahtjevno.

Blockchain mreža se sama po sebi smatra kao dobrim rješenjem u opskrbnim lancima baš zato što nudi zajedničku i nepromjenjivu bazu podataka, transparentnu, sigurnu i decentraliziranu platformu.
Instalacija pametnih ugovora omogućuje automatiziran i siguran protok informacija dok svaki sudionik ima službenu identifikaciju i može sudjelovati u validaciji transakcija. Transakcije se tako mogu pratiti od strane svih sudionika u lancu opskrbe u realnom vremenu.

Kada je riječ o korištenju Fabric platforme u kontekstu lanca opskrbe, njegova modularna priroda predstavlja idealno rješenje za neke od problema koje susrećemo u tradicionalnim Blockchain sustavima. Mogućnost stvaranja kanala unutar privatne mreže predstavlja veliku prednost što se tiče samih podataka. Sudionici nekog kanala mogu imati uvid u cijene ili ponude koje konkurentske organizacije ne smiju vidjet. Činjenica da je identitet svih sudionika poznat, predstavlja dodatnu funkcionalnost u odnosu na monolitsku strukturu klasičnog Blockchaina. Možda i najbitnija karakteristika kod primjene Fabric mreže unutar lanca opskrbe je njegova brzina izvedbe transakcija, zahvaljujući mogućnosti stvaranja konsenzusa po mjeri i paralelno izvođenje transakcija.
Primarna uloga Fabric aplikacija je u praćenju robe i imovine. Može se istaknuti kako je riječ o kontrolnoj funkciji, ali i funkciji planiranja te upravljanja imovinom. Korištenjem platforme dobiva se uvid u proces, koji kreće od proizvodnje preko transporta pa sve do potrošnje, odnosno tržišnog plasmana i kupovine. U skladu s time, Fabric može podržavati sve faze nabave, a sam proces postaje učinkovitiji, kvalitetniji i stabilniji. Funkcionalnoisti koje pruža Fabric mreža može se prikazati na sljedeći način (Tablica 2.).

Tablica 1. Hyperledger Fabric u lancu opskrbe

Upravljanje članstvom	Potvrditelj članstva provjerava autentifikaciju, autorizaciju i upravlja identitetom, te odobrava članstvo.
Digitalni potpis	Kriptografska validacija identiteta za sve dionike.
Naručivanje	Naručitelj usluga vrši naručivanje transakcije preko čvorova do svih korisnika, članova.
Vremenske oznake	Bilježenje transakcija i radnji u realnom vremenu.
Nepromjenjivost natječajnog dokumenta	Pohranjivanje čvora i podataka na bloku koji je nepromjenjiv.
Ugovaranje	Digitalno ugovaranje i ovjera od strane sukladnih dionika/članova.
Plaćanje	Sigurno okruženje za mikro plaćanje.
Interni podaci i upravljanje	Osiguranje potpune sigurnosti podataka i upravljanja istima
Interoperabilnost	Interoperabilnost među članovima i organizacijama.
Sigurnost	Provjere, konsenzusi, autentifikacija.

Izvor: Nodehi, T. i dr.(2020.) A Blockchain Based Architecture for Fulfilling the Needs of an E-Procurement Platform. Dostupno na: http://www.ieomsociety.org/detroit2020/papers/64.pdf (05.06.2022.).

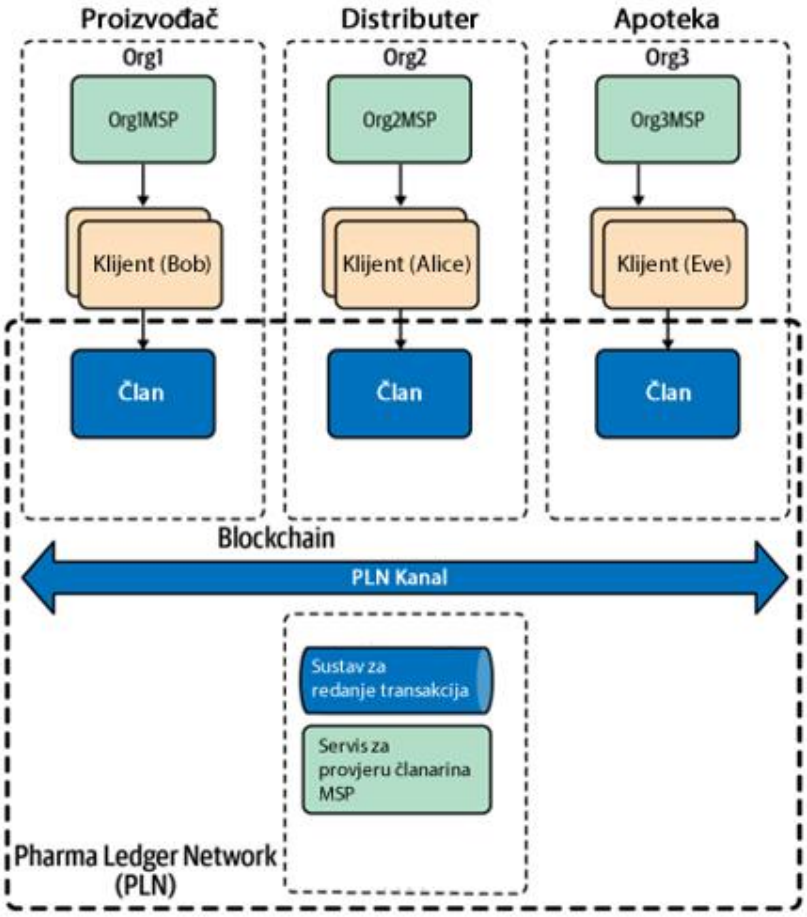
Prema navedenim funkcionalnostima Fabric mrežu možemo primijeniti na razne slučajeve upotrebe. Stvaranje kompleksnih platformi za nabavu sirovina u auto industriji je samo jedan od njih. Tu se mogu povezati razne organizacije i vršiti sigurnu kupoprodaju kroz dinamičke sustave aukcija ili obrnutih aukcija. Druga primjena može biti u prehrambenoj industriji gdje je jako bitno poznavati i garantirati identitet sudionika

(Deloitte, 2017). U nastavku ovog rada predstavljena je primjena Fabric mreže u lancu nabave lijekova u farmaceutskoj industriji, kao primjer platforme čija je svrha detaljno praćenje proizvoda radi garantiranja porijekla i sprječavanja manipulacije sadržaja lijekova.

3.3.1. UPRAVLJANJE OPSKRBOM LIJEKOVA

Prema podacima svjetske zdravstvene organizacije, procijenjeno je da se godišnje na svjetsko tržište plasira preko 200 milijardi dolara vrijedno krivotvorenih lijekova, od čega se 50% prodaje obavi online. Lijekovi se najčešće krivotvore već u koraku proizvodnje, a mogu bit zamijenjeni lažnim primjercima dok ne dođu do krajnjeg odredišta (Deloitte, 2017). Upravo bi stvaranje Blockchain mreže predstavljalo idealno rješenje u borbi praćenja autentičnosti lijekova, pružajući uvid u cjeloukupni lanac opskrbe lijeka, od njegove proizvodnje do krajnjeg korisnika.
Koristeći se raznim vrstama senzora u proizvodnom lancu, podaci se mogu u realnom vremenu bilježiti unutar pametnih ugovora koji će automatski pokrenuti odgovarajuće radnje. U slučaju da podaci nisu prihvatljivi, nepravilnost se može odmah javiti odgovornoj ustanovi i lijek se može odbaciti. Odgovorne ustanove imaju tako uvid u legitimnost cijelog sustava koji predstavlja garanciju i za sve ostale sudionike, jer svatko može kontrolirati čitavu povijest proizvoda kroz nepromjenjivu bazu podatak (Deloitte, 2017).
U primjeru koji slijedi u nastavku (Slika 10.), prikazan je jednostavan model lanca opskrbe lijekovima u kojem su prikazana tri sudionika. Krenuvši od proizvođača, distributera pa do apoteke kao krajnjeg korisnika.

Slika 10. Pharma Ledger Network udruženja u lancu opskrbe lijekova.



Izvor: Izrađeno prema Zand M. (2021) Hands-On Smart Contract Development with Hyperledger Fabric V2, O'Reilly. Str. 144.

Svaki od ta tri sudionika predstavlja organizaciju za sebe i zajedno formiraju zajedničko udruženje ili konzorcij. Unutar organizacija i udruženja članovi mogu kreirati korisnike, kreirati i prizivati pametne ugovore i pretraživati zajedničke podatke.

Udruženje organizacija u primjeru nazvan je “Pharma Ledger network” i svaka organizacija ima jednog korisnika sučelja aplikacije, jednog člana (engl. Peer) i sustav za provjeru identifikacije (engl. Membership Service Provider – MSP). Ime korisnika sučelja aplikacije za proizvodnju je Bob, Alice je korisnik sučelja aplikacije distributera i Eve je naziv korisnika sučelja aplikacije unutar apoteke.
Sustav za redanje transakcija (engl. Orderer) ima vlastiti sustav za validaciju identiteta MSP i zajedno sa tri prethodno navedene organizacije čini privatni kanal komunikacije

pod nazivom Plnchannel. Kroz taj se kanal onda vrši egzekucija i validacija transakcija (Zand i dr., 2021).

3.3.2. PLAN TIJEK LIJEKOVA U LANCU OPSKRBE

Naš se jednostavni lanac opskrbe lijekova sastoji od tri koraka, proizvodnje proizvoda, distribucije i konačna dostava u apoteci. U nastavku slijedi detaljniji prikaz cijelog procesa kojeg možemo prikazati kroz sljedeće korake:

- Prvi korak zahtjeva da je svaki član registriran i da ima valjanu identifikaciju unutar mreže. Certifikat kod svake organizacije posebno izdaje Fabric centar za generaciju identiteta (engl. Fabric Certificate Authority - CA). Jednom kada je identifikacija kreirana, članovi mogu međusobno komunicirati.
- Proizvođač u trenutku kreacije novog proizvoda, poziva kroz aplikaciju pametni ugovor zaslužan za kreaciju zapisa o informacijama o proizvodu i šalje mu početne vrijednosti.

  Pametan ugovor je u našem slučaju instaliran na svim članovima konzorcija i svi provjeravaju ispravnost podataka i identitet proizovđača jer smo tako definirali u politici za konsenzus.

  Ako je valjanost podataka i identiteta proizvođača ispravna, generira se simulacija zapisa sa informacijama o proizvodu i šalje se natrag do klijenta koji provjerava digitalni potpis članova koji su izvršili simulaciju i odobrili je. Ako je konsenzus ispunjen tako što su svi priznali ispravnost podataka, podaci se šalju članu za redanju transakcija koji formira blok i šalje ga na ponovnu validaciju svim članovima organizacija. Članovi nakon druge validacije ako je sve ispravno zapisuju blok u Blockchain i ažuriraju bazu podataka stanja.

  U našem primjeru kreiran je novi proizvod s jedinstvenim identifikacijskim brojem 2000.001.

  Podaci o novom proizvodu, proizvođaču, vremenskim oznakama i statusu vlasništva stvaraju zapis kojeg upisujemo unutar Blockchaina (Slika 11).

Slika 11. Prikaz informacija o proizvodu kod proizvođača.

Izvor: Izrađeno prema Zand M. (2021) Hands-On Smart Contract Development with Hyperledger Fabric V2, O'Reilly. Str. 145.

- Nakon nekoliko tjedana gotov se proizvod šalje dobavljaču koji prilikom zaprimanja proizvoda mora ažurirati zapis o vlasništvu i upisati sebe (Slika 12).

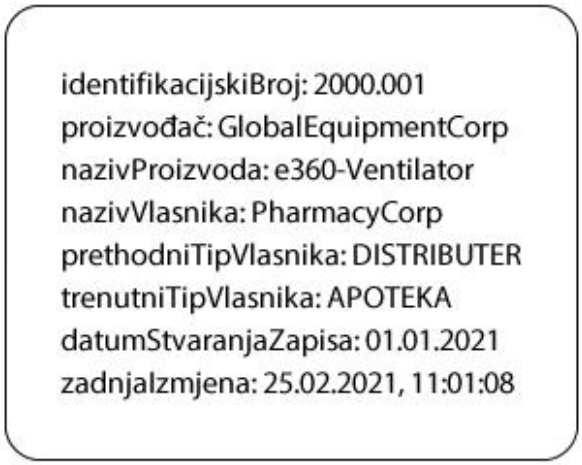
Slika 12. Prikaz informacija o proizvodu kod distributera.

Izvor: Izrađeno prema Zand M. (2021) Hands-On Smart Contract Development with Hyperledger Fabric V2, O'Reilly. Str. 145.

Ponovno se pokreće jednak proces validacije i konsenzusa kao i u slučaju kada je informacije o vlasništva proizvoda upisivao proizvođač. Iz novog zapisa je točno vidljivo kod koga se trenutno nalazi proizvod, kod koga je bio prethodno i kada se desila zadnja izmjena.

- Nakon mjesec dana proizvod stiže od distributera u apoteku. Sukladno promjeni vlasništva, na jednak način zajedničkim konsenzusom dodajemo novo stanje o proizvodu u blockchain koji će sada imati kao status vlasništva, apoteku (Slika 13).

Slika 13. Prikaz informacija o proizvodu kod apoteke.



Izvor: Izrađeno prema Zand M. (2021) Hands-On Smart Contract Development with Hyperledger Fabric V2, O'Reilly. Str. 146.

U ovom našem pojednostavljen primjeru Fabric mreže mogu se priključiti dodatni sudionici, kao što su kupci lijekova i neutralne komisije za provjeru ispravnosti proizvoda. Oni mogu imati ograničeni pristup mreži i uvid samo na određene podatke, ali dovoljno za procjenu o autentičnosti proizvoda. U slučaju neke neispravnosti, lako je utvrditi na kom se mjestu desila i kada.

3.4. OSTALE USPJEŠNE PRIMJENE

Poznati trgovački lanac Walmart je uvijek pokazivao interes u stvaranju transparentne mreže radi praćenja namirnica. Brojne su situacije u kojima se desi da se na policama trgovine plasira pokvareni proizvod, te je za pronalazak njegovog porijekla potrebno nekoliko tjedana. U tom se dužem razdoblju izgubi kredibilitet proizvoda ili pak čitavog branda, a posljedice mogu biti još i veće jer se zna izolirati čitavo područje proizvodnje pokvarenog proizvoda dok se ne pronađe štetni izvor, što ugrožava i nedužne proizvođače u toj zoni.

Hyperledger Fabric kao platforma predstavljao je najbolju opciju zbog toga što se radi o slobodno softveru (engl. Open-source). Upravo u prehrambenom lancu opskrbe to predstavlja veliku prednost zbog velikog broja sudionika i daje priliku svakome da se uz minimalne troškove uključuju u razmjenu podataka.

Walmart je započeo s jednostavnim projektima kao što su praćenja manga u lancu opskrbe i stvaranje certifikata za autentičnost i kvalitetu svinjetine na kineskom tržištu. U prve dvije godine korištenja platforme Walmart je uspio pokrenuti praćenje 25 proizvoda od 5 različitih proizvođača. Jedan od razloga uspješnosti je bilo zasigurno ubrzavanje čitavog procesa dokazivanja porijekla namirnice sa prethodnih 7 dana na samo 2.2 sekunde.

Zajedno sa IBM-om osnovali su kompleksniji lanac praćenja proizvoda pod nazivom „IBM Food Trust“ kojeg žele angažirati za praćenje svog svježeg povrća u bliskoj budućnosti (Hyperledger.org, pristup 01.07.2022).

Tvrtka Honeywell Aerospace uspjela je oživiti trgovinu rabljenih dijelova korištenih u avijaciji.

Riječ je o trgovini koja se pretežito vršila direktnim kontaktom i zahtijevala je nekolicinu telefonskih poziva ili e-mailova da se privede kraju. Online trgovine koje su do sada postojale izgledale su jako rudimentarno i sadržavale su jako malo podataka o proizvodu za industriju koja zahtijeva visoki standard preciznosti. Osim potrebom za detaljnim opisom proizvoda, povjerenje između prodavača i kupca igra važnu ulogu, a još su više potrebni certifikati koje zahtijevaju razne ustanove za svaku komponentu koju će kupac morati ugrađivat u svoju letjelicu.

Iduću prepreku predstavlja velika količina podataka koja se treba sigurno spremiti. Prosječni avion ima vijek korištenja od 30 godina, pet ili šest vlasnika i sačinjen je od

preko 4 milijuna komponenti.
Ovu kompleksnost podataka zahtjeva sustav koji će sve to voditi efikasno i bez greške.

Zbog svih tih zahtjeva, uspjeli su osnovati platformu za trgovanje zamjenskih komponenti u avijaciji pod nazivom “GoDirect Trade”. Osnovana je na osnovi Hyperledger Fabric platforme i osigurava praćenje životnog ciklusa komponenti, broj radnih sati za svaku komponentu, uvid u povijest kvarova i popravka i sve prijašnje vlasnike za svaku komponentu.
Ovakva vrsta platforme ima i pozitivni ekološki utjecaj jer pomaže u recikliranju starih letjelica, na Kojima se u prosjeku može ponovno iskoristiti preko 1000 dijelova.
GoDirect trade pokazala je jako veliku zainteresiranost korisnika, tako što je u prvoj godini korištenja privukla trećinu potencijalnih korisnika iz čitave branše, gotovo 5000 korisnika (Hyperledger.org, pristup 01.07.2022).

Fabric platformu možemo primijeniti na mnogobrojne slučajeve koji ne moraju biti striktno vezani za lanac opskrbe. Mindtree je uspio stvoriti platformu pod nazivom “$wap” koja predstavlja jedinstveni program lojalnosti kupaca (engl. Loyaliti program) u kojem se razne organizacije koje izdaju bodove mogu ujediniti i međusobno dijeliti iste. Procjenjuje se da godišnje ostane neiskorišteno preko 100 milijardi dolara skupljenih bodova kroz razne programe lojalnosti kupaca. Kroz aplikaciju $wap, organizacije se puno brže mogu učlaniti i imati uvid u realnom vremenu o aktivnostima kupaca (Hyperledger.org, pristup 02.07.2022).

ZAKLJUČAK

Ako promatramo različite poslovne modele elektroničke trgovine unutar lanca opskrbe, B2B model predstavlja možda primjer modela poslovanja s naj kompleksnijom strukturom koji ima još puno prostora za napredak. Zbog raznih sudionika u samom procesu, teško je kreirati standardiziran model podataka u kratkom razdoblju kojeg će prihvatiti svi članovi uz minimalni napor implementacije. Upravo je stvaranje platforme standardiziranih i sigurnih podataka najveći problem unutar B2B poslovnih modela, jer ne stignu pratiti tehnološke trendove zbog njihove kompleksnosti. Primjer ovog usporenog trenda je standardiziran sustav elektroničke razmjene podataka (EDI) koji je nastao 70-ih godina i opstao do dan danas. Poseban doprinos u kontekstu upravljanja i nadzora procesa lanca opskrbe vidljiv je kod Blockchain tehnologije. Decentralizirana i nepromjenjiva baza podataka predstavlja ključnu prednost u odnosu na tradicionalne modele pohrane podataka, tako da se ukida svaki posrednik, smanjuje pogreška i daje naglasak na transparentnost. Sve je to izvedivo kombinacijom tehnologija kao što su peer-to-peer mreže, funkcije hashiranja, binarna stabla i digitalni potpisi. Ujedinjenjem ovih legacy tehnologija, stvorili su se temelji za kreaciju rješenja unutar raznih industrija. Elektronička trgovina u lancu opskrbe je sigurno jedna od branši koja može imati velike koristi od Blockchain tehnologije, ali uz potrebne dorade. Pametni ugovori su još jedan od rješenja prisutnih u klasičnim Blockchain mrežama koji mogu omogućiti automatizaciju kompleksnih procesa u lancu opskrbe, ali još uvijek nedovoljno da pokri sve zahtjeve potrebne da veći broj organizacije postigne zajedničke ciljeve. Iz tog su se razloga razvijale razne Blockchain platforme modularnih arhitektura koje dozvoljavaju da se određeni sustavi elektroničke trgovine kroje po mjeri. Upravo je Hyperledger Fabric jedna od tih platformi privatne Blockchain mreže koja omogućuje prisustvovanje odabranih i opće poznatih sudionika za koje su točno definirane uloge unutar mreže. Fabric se bazira na execute-order-validate arhitekturi koja omogućuje paralelno izvođenje transakcija što doprinosi znatnom napretku u performansama. Uz fleksibilnu politiku konsenzusa valjanosti transakcija može se zaključiti da ova platforma pogoduje svim izravno i neizravno povezanim sudionicima.

LITERATURA

Knjige:

- Panian, Ž. (2013) Elektroničko poslovanje druge generacije, Ekonosmki fakultet Zagreb.
- Radovilsky i dr., (2015) Business Models for E-Commerce, 2015 California State Univerity, East Bay
- Ružić, D. i dr. (2014.) E-marketing. Osijek: Factum d.o.o.
- Spremić M (2004.) Menadžment i elektroničko poslovanje. Zagreb: Narodne novine
- Spremić, M. (2017) Digitalna transformacija poslovanja, Ekonosmki fakultet, Zagreb
- Van Weele, A.J. (2014.) Purchasing and Supply Chain Management, South-Western Cengage Learning, Hampshire, UK.
- Zand, M. (2021) Hands-On Smart Contract Development with Hyperledger Fabric V2, O'Reilly

Članci:

- Deloitte, (2017) Supply chain meets Blockchain. Dostupno na: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-supply-chain-meets-blockchain.pdf (30.06.2022)
- Jaklic, J. i dr. (2006.) Enhancing lean supply chain maturity with business process
- Nodehi, T. (2020) A Blockchain Based Architecture for Fulfilling the Needs of an E-Procurement Platform. Dostupno na: http://www.ieomsociety.org/detroit2020/papers/64.pdf (30.06.2022)

Internet izvori:

- Actualide de Commerce (2022.) Elektronička trgovina. Dostupno na: https://www.actualidadecommerce.com/hr/que-es-e-commerce/ (31.05.2022.)
- Cardanians.io (2019) Diving into Protocol Consensus. Dostupno na: https://cardanians-io.medium.com/diving-into-protocol-consensus-1343f7f42fc6 (21.06.2022)
- CARNET, (2007) Digitalni potpis. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf (25.06.2022)
- CARNET (2009) Peer-to-peer mreže. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2009-11-282.pdf (02.06.2022)
- Dzikowski, J. Hyperledger Fabric Cheat Sheet. Dostupno na: https://softwaremill.com/hyperledger-fabric-cheat-sheet/ (23.06.2022)
- FER, (2017) Raspodijeljeni sustavi. Dostupno na: https://www.fer.unizg.hr/_download/repository/RS-2017_13.pdf (10.06.2022)
- Frankenfield, J. (2021) Decentralized Applications (dApps). Prisutno na: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp (25.06.2022)
- Frankenfield, J. (2022) Hash. Dostupno na: https://www.investopedia.com/terms/h/hash.asp (20.06.2022)
- Geeksforgeeks.org (2022) practical Byzantine Fault Tolerance(pBFT). Dostupno na: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/ (23.06.2022)
- Github.io, Smart Contracts and Chaincode. Dostupno na: https://hyperledgendary.github.io/unstable-fabric-docs/smartcontract/smartcontract.html (25.06.2022)
- Hamill, C. (2022) Razumijevanje digitalnih potpisa u blokčejnu i kako to funkcionira. Dostupno na: https://morioh.com/p/6758c95ab0b3 (25.06.2022)
- Hejduk, G. (2021) Channel, one of the key abstractions in Hyperledger Fabric — what is it for?. Dostupno na: https://softwaremill.com/channel-one-of-the-key-abstractions-in-hyperledger-fabric-what-is-it-for/ (05.06.2022)

- Hyperledger.org, Honeywell case study. Dostupno na: https://www.hyperledger.org/wp-content/uploads/2019/12/Hyperledger_CaseStudy_Honeywell_Printable_12.12.19.pdf (02.07.2022)
- Hyperledger.org, Mindtree case study. Dostupno na: https://www.hyperledger.org/wp-content/uploads/2020/06/Hyperledger_CaseStudy_Mindtree_Printable.pdf (02.07.2022)
- Hyperledger.org, Walmart case study. Dostupno na: https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf (02.07.2022)
- IBM.com, Smart contracts defined. Dostupno na: https://www.ibm.com/topics/smart-contracts (12.06.2022)
- IBM, (2018) Behind the Architecture of Hyperledger Fabric. Dostupno na: https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/ (27.06.2022)
- Kathleen, E. (2021) Types of Blockchain: Public, Private, or Something in Between. Dostupno na: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between (10.06.2022)
- Kumar, S. (2018) The Ultimate Guide to Consensus in Hyperledger Fabric. Dostupno na: https://www.skcript.com/svr/consensus-hyperledger-fabric/ (06.06.2022)
- Mancini, B. (2020) Merkle Tree Construction and Proof-of-Inclusion. Dostupno na: https://www.derpturkey.com/merkle-tree-construction-and-proof-of-inclusion/ (12.06.2022)
- Medium.com, Hyperledger Fabric components. Dostupno na: https://osintiostom.medium.com/hyperledger-fabric-components-f8978a53279c (15.06.2022)
- Moralis.io EVM Explained – What is Ethereum Virtual Machine? Dostupno na: https://moralis.io/evm-explained-what-is-ethereum-virtual-machine/ (19.06.2022)

- Mycointainer.com (2020) Proof of Stake: Crypto Staking Vs. Crypto Minting. Dostupno na: https://www.mycointainer.com/insight/proof-of-stake-crypto-staking-vs-crypto-minting/ (21.06.2022)
- Radosevic, R. (2018) Kako će Blockchain promijeniti vaš lanac opskrbe i cijelu logističnu industriju. Dostupno na: https://dario-dr.medium.com/kako-%C4%87e-blockchain-promijeniti-va%C5%A1-lanac-opskrbe-i-cijelu-logisti%C4%8Dnu-industriju-5d1aaaa6fabd (12.06.2022.)
- Readthedocs.io, Identity. Dostupno na: https://hyperledger-fabric.readthedocs.io/en/release-2.2/identity/identity.html (15.06.2022)
- Readthedocs.io, membership. Dostupno na: https://hyperledger-fabric.readthedocs.io/en/release-2.2/membership/membership.html (15.06.2022)
- Readthedocs.io, The Ordering Service. Dostupno na: https://hyperledger-fabric.readthedocs.io/en/latest/orderer/ordering_service.html (04.06.2022)
- Rilee, K. (2018) Understanding Hyperledger Fabric — Gossip. Dostupno na: https://medium.com/kokster/understanding-hyperledger-fabric-gossip-512a217d5d1e (15.06.2022)
- Saraswat, N. (2018) Difference between distributed ledger technology and blockchain. Dostupno na: https://medium.com/sodio-tech/difference-between-distributed-ledger-technology-and-blockchain-1cfada83cc12
- Tutorialandexample, (2022) Blockchain Merkle Tree. Dostupno na: https://www.tutorialandexample.com/blockchain-merkle-tree (12.06.2022)
- Zhao, H. (2018) hash pointers and dana Structures. Dostupno na: https://zhaohuabing.medium.com/hash-pointers-and-data-structures-f85d5fe91659 (12.06.2022)

POPIS SLIKA

Slika 1. Odnosi u elektroničkoj trgovini 4

Slika 2. Prikaz strukture podataka unutar blokova 7

Slika 3. Prikaz vezanja i stvaranja neizmjenjivog lanca blokova 8

Slika 4. Prikaz Merkleovog stabla 10

Slika 5. Shematski prikaz postupka stvaranja i provjere digitalnog potpisa 12

Slika 6. Sastavnih dijelova za pohranu podataka unutar članova i kanala 21

Slika 7. Order-execute Blockchain proces izvođenja transakcija 25

Slika 8. Tijek execute-order-validate Fabric procesa izvođenja transakcija 26

Slika 9. Transakcijskog proces unutar Hyperledger Fabric mreže 27

Slika 10. Pharma Ledger Network udruženje u lancu opskrbe lijekova 31

Slika 11. Prikaz informacija o proizvodu kod proizvođača 33

Slika 12. Prikaz informacija o proizvodu kod distributera 33

Slika 13. Prikaz informacija o proizvodu kod apoteke 34

POPIS TABLICA

Tablica 1. Hyperledger Fabric u lancu opskrbe 29