DOI 10.7251/ZRPIM2001344M

STRUČNI RAD – PROFESIONAL PAPER

IZBOR BLOCKCHAIN TEHNOLOGIJE ZA IMPLEMENTACIJU SOFTVERSKOG REŠENJA U SPECIFIČNOJ OBLASTI USLUGA ILI INDUSTRIJE

Vladimir Milićević, Igor Franc, Andrija Đurić

[1]Univerzitet Metropolitan, Tadeuša Košćuška 63, 11 158 Beograd, Srbija,
vladimir.milicevic@metropolitan.ac.rs

APSTRAKT

U savremenoj softverskoj industriji, koja je u konstantnoj ekspanziji, problem poverenja između različitih korisnika softverskog rešenja postaje sve više dominantan. Krajnji korisnici žele da budu u potpunosti sigurni da je proizvod ili usluga u potpunosti usaglašena sa njihovim zahtevima i da kvalitetom ne odstupa od izabranog ili naručenog proizvoda ili usluge. Proizvođači ili pružaoci usluga, sa druge strane žele da imaju potpunu informaciju u vezi sa kvalitetom sirovina ili infrastukturom koju obezbeđuju sa ciljem kreiranja proizvoda i usluge, a koje bi trebalo da im obezbedi odgovarajući dobavljač. Svi učesnici u softverskom rešenju (aktori) kao imperativ imaju i sigurnost vlastitih podataka koji se čuvaju, obrađuju i razmenjuju unutar uvakvog jednog softverskog sistema.

Cilj rada je demonstracija primene inovativnog pristupa u čuvanju, obradi i razmeni informacija upotrebom blockchain tehnologije sa studijom slučaja na lancu snabdevanja. Postoje različiti pristupi i u prvom koraku biće poređeni odgovarajući: Ethereum i Hyperledger Fabric blockchain mreža/platforma. Nakon izbora odgovarajuće tehnologije rad će se fokusirati na ispitivanje potencijalnih sigurnosnih rešenja koje blokčejn tehnologija omogućava za potrebe slučaja korišćenja. To znači da je prvenstveno potrebno objasniti potrebne koncepte blockchain tehnologije, a zatim napraviti model slučaja korišćenja, detaljno ga opisati i produbiti do adekvatne mere za ispitivanje, i konačno testirati nad njim neke hipoteze vezane za poboljšanje transparentnosti, integriteta informacija, održavanje sigurnosti mreže sistema, održavanje efektivnih inicijativa za učestvovanje i odbranu od loših motivacija svih aktera unutar sistema.

Ključne reči: blockchain, softverski sistem, platforma, poverenje, učesnici.

UVOD

Blockchain, kao mlada tehnologija, sve više uzima maha u različitim oblastima proizvoda i usluga servisiranih savremenim sofverskim rešenjima, baziranim na inteligentnim mehanizmima. Blockchain je već naišao na primenu u brojnim aplikacijama, izgrađenim na različitim domenima, kao decentralizovani pristup razvoju i primeni softvera otpornog na prevare, bez poverenih autoriteta. Blockchain je distribuirani, skup vremenski obeleženih zapisa, u koje je moguće samo upisivanje novih podataka i koji je kriptografski zaštićen od neovlašćenog pristupa i revizije (Nakamoto, 2009). Ovako mlada, ali veoma perspektivna tehnologija, naišla je na primenu u oblastima poput (Chen et al, 2018):

- kriptovaluta,
- sistema zdravstvene zaštite,
- sistema osiguranja,
- sistema oglašavanja,
- zaštite autorskih prava,
- energije,
- rastućem IoT sektoru,

- bankarstvu,
- društvenim mrežama, i tako dalje.

Primena ovakve tehnologije ima za cilj povećanje nivoa zadovoljstva korisnika sistema kroz veći stepen poverenja u softversko rešenje koje uvažava svu privatnost učesnika, ali i odgovarajuću zakonsku regulativu vezanu za oblast u kojoj se softver primenjuje (Bayon, 2019).

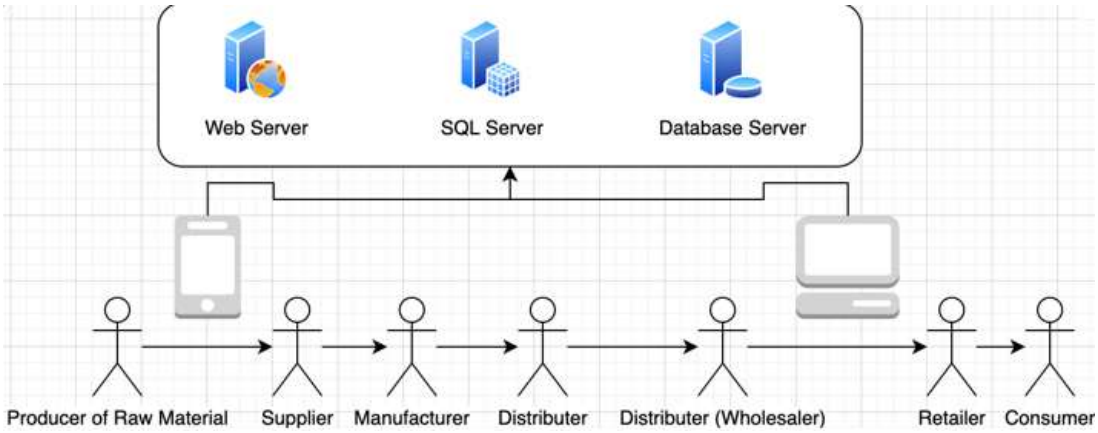
Cilj ovog rada je analiza i diskusija izbora odgovarajuće blockchain tehnologije kao i ispitivanje njene primenljivosti za osiguravanja informacija u sistemima upravljanja lancima snabdevanja (Tribis et al, 2018).

Danas već postoje informacioni sistemi za podršku lancima snabdevanja. Ovakvi softverski sistemi rešavaju neke logističke probleme na tradicionalni način tj. korišćenjem centralizovane ili do neke mere distribuirane softverske arhitekture. Ovaj način je omogućio da sistemi upravljanja lancima snabdevanja (u digitalnoj formi i korišćenjem nekog softverskog rešenja kupovinom ili kreiranjem vlastitog softverskog rešenja) nude poslovna poboljšanja u odnosu na prethodni način rukovođenja lancem snabdevanja pre uvođenja računarske podrške.

Poboljšanja u odnosu na upravljanje lancem snabdevanja pre dolaska i napretka softverskih sistema su sledeća:

- Lakše prenošenje informacija preko aplikacija i serverskih poziva unutar celokupnog sistema lanca snabdevanja.
- Centralizovano praćenje stanja i istorije lanca snabdevanja.
- Digitalni signal je sigurniji od papira u smislu integriteta podataka, poverljivosti informacija kroz heširanje i enkripciju.
- Lakše i potencijalno jeftinije umrežavanje manjih i srednjih preduzeća u poslove i sistem lanca snabdevanja.

Na slici 1 je prikazan primer tradicionalnog informaciono tehnološkog (IT) SCM (Supply Chain Management) sistema:



Slika 1. Tradicionalni IT sistem za upravljanje lancem snabdevanja

Slika pokazuje da u centralizovanom SCM sve informacije se šalju centralizovanoj komponenti koja ih čuva i prosleđuje u lancu snabdevanja.

Postoje određeni problem vezani za primenu tradicionalnih softverskih SCM sistema:

- Manjak transparentnosti za sve aktere i/ili krajnje korisnike lanca snabdevanja.
- Ignorisanje pojedinih, potencijalno korisnih informacija lanca snabdevanja.
- Teža provera potencijalnih ljudskih grešaka u lancu ili transakcijama između poslovnih partnera.

- Poslovni partneri ne veruju jedni drugima i prave "informaciona ostrva" umesto da su potencijalno umreženi; time je protok informacija sporiji i ograničeniji.
- Automatizovano praćenje odgovornosti.

Postavlja se pitanje, da li je moguće sigurnosno unaprediti SCM u odnosu na dosadašnji način funkcionisanja i kreiranja takvih sistema - tako da je poslovno održiv i izvodljiv sistem za upravljanje lancem snabdevanja? Blockchain je moguće rešenje ovog problema!

IZBOR BLOCKCHAIN TEHNOLOGIJE

Pre nego što razvojni tim krene u razvoj softverskog rešenja koje inkorporira blockchain za čuvanje i vođenje poslovnih transakcija, neophodno je da se do detalja upozna sa blockchain konceptima, tehnologijama i alatima koji će omogućiti povezivanje poslovanja sa savremenom tehnologijom. Posebno je važno odabrati pravu blockchain tehnologiju da bi koristi poslovanja nakon implementacije ovakvog rešenja bili maksimizovani. Postoje brojna tehnološka rešenja ali se posebno ističu dva: Hyperledger i Ethereum, između kojih je potrebno izabrati onu koja se najbolje uklapa u zahteve za kreiranje softverskog rešenja.

Za izbor odgovarajuće blockchain tehnologije neophodno je identifikovati određene kriterijume za izbor. Predlažu se sledeće veličine kao kriterijumi izbora adekvatne blockchain tehnologije za implementaciju informacionog sistema za podršku procesu lanca snabdevanja:

- svrha konkretne blockchain tehnologije;
- poverljivost;
- tip privatnosti mreže;
- primenjeni mehanizam konsenzusa;
- podržani programski jezici;
- podrška za kriptovalute.

Sledećom tabelom su prikazane ključne razlike između Hyperledger i Ethereum blockchain platformi po prethodno navedeni kriterijumima.

Tabela 1. Ključne razlike između Hyperledger i Ethereum blockchain platformi (www.edureka.co)

Karakteristika	Hyperledger	Ethereum
Svrha	Preferirana platforma za B2B poslovanje	Platforma za B2C poslovanje i opštu primenu
Poverljivost	Poverljive transakcije	Transparentno
Vrsta mreže	Privatna - bazirana na dozvolama	Javna / privatna - bazirana na dozvolama
Mehanizam konsenzusa	Veći izbor: Nije potrebno miniranje	POW algoritam: postiže se rudarenjem
Programski jezik	Kod lanca napisan u GO ili Java jeziku	Pametni ugovori napisani u Solidity
Kriptovaluta	Nema podršku	Ugrađena kriptovaluta Ether

Pre identifikovanja odgovarajuće tehnologije, neophodno je obaviti dodatnu analizu i diskusiju, a pre svega upustiti se u jasno identifikovanje šta zapravo Hyperledger i Ethereum predstavljaju.

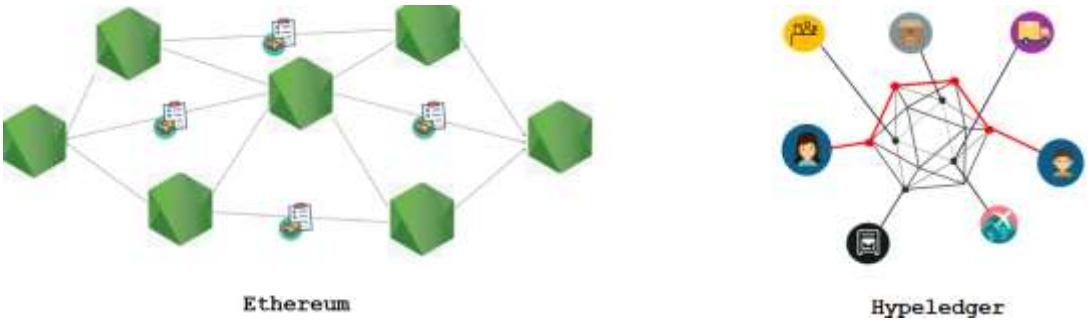
Ethereum je predstavlja javnu distribuiranu blockchain mrežu baziranu na principima otvorenog koda (open source). Nad sobom dozvoljava izgradnju decentralizovanih aplikacija uz upotrebu funkcionalnosti poznate pod nazivom pametni ugovori (smart contracts). Već sada je moguće sagledati brojne relevantne informacije vezane za primenu pametnih ugovora u brojnoj štampanoj i elektronskoj literaturi. (Kosba et al, 2016, Idelberger et al, 2016, Alharby et al, 2017).

Ethereum je razvio Vitalik Buterin kao nadogradnju na originalno jezgro blockchain koncepta (Metcalfe, 2020). Autor je korigova Bitkoin protokole omogućivši tako podršku za aplikacije koje se razvijaju bez prvenstvenog oslanjanja na kriptovalute. Glavni doprinos uvođenja ove platforme ogleda se u razvoju koncepta pametnih ugovora. Pametni ugovori su delovi koda koji se izvršavaju na mreži. Otuda, ova platforma omogućava programerima pisanje programa za podršku decentralizovanim organizacijama.

Bilo ko na globalnoj mreži može da pristupi Ethereum blockchain mreži i na taj način postane i sam učesnik mreže. Otuda, Ethereum je poznat i pod nazivom „Svetski računar“ (World Computer) (izvor: www.abra.com).

„Hyperledger je razvojni projekat otvorenog koda koji koristi ekosistemu dobavljača i korisnika rešenja zasnovanih na Hyperledger-u. Fokusiran je na slučajeve upotrebe koji se odnose na blockchain tehnologiju i koji imaju primenu u različitim industrijskim sektorima“ (Brian Behlendorf , izvršni direktor Hyperledger-a). Za razliku od Ethereum-a, Hyperledger nudi veću slobodu programerima za razvoj personalizovanih blockchain mreža koje se uklapaju u konkretne potrebe poslovanja. Hyperledger se, otuda, ne može smatrati alatom ili platformom poput Ethereum-a, već strategijom koja obuhvata različite platforme za razvoj kompleksnih (enterprise) softverskih rešenja koja obuhvataju blockchain tehnologije.

Slikom 2 je dat jednostavan vizuelni opis mreža Ethereum i Hyperledger.



Slika 2. Jednostavan vizuelni opis mreža Ethereum i Hyperledger

Nastavlja se dalje diskusija u smeru izbora odgovarajuće blockchain tehnologije za izgradnju softverskog rešenja za podršku lancu snabdevanja.

Ethereum pokreće pametne ugovore na virtuelnim mašinama za aplikacije koje su decentralizovane i namenjene za masovnu upotrebu. Sa druge strane, Hyperledger pokriva blockchain tehnologije za direktnu podršku poslovanju. Dizajniran je da podrži prilagodljive implementacije komponenti koje pružaju visok stepen poverljivosti, otpornosti i skalabilnosti. Hyperledger ima modularnu arhitekturu i pruža veliku fleksibilnost kada je njegova upotreba u pitanju. Po ovom kriterijumu za lance snabdevanja je pogodnija upotreba rešenja baziranih na Hyperledger-u.

Ako se nastavi diskusija u smeru poverljivosti, Ethereum-ova transparentnost, takođe, dovodi do toga da za konkretne scenarije upotrebe, u aplikacijama za podršku lancima snabdevanja, bolje je primeniti rešenja bazirana na Hyperledger-u. Dok je u Ethereum-u svaka transakcija dostupna svim učesnicima na mreži, u Hyperledger-u su transakcije poverljive i dostupne samo onim učesnicima koji poseduju odgovarajuću enkripcijski ključ za pristup transakciji.

Takođe, privatnost Hyperledger-a omogućava da u ovakvom tipu mreže mogu da učestvuju samo oni akteri sa predefinisanim pravima pristupa.

U blockchain mrežama odluke se donose na osnovu mehanizma konsenzusa. Ethereum koristi mehanizam konsenzusa putem rudarenja baziranog na Proof-of-Work (PoW) algoritmu (Sarkar, 2020). To znači da svi čvorovi u mreži moraju da postignu konsenzus nad svim učinjenim transakcijama. Hyperledger ima preciznu kontrolu nad konsenzusom i ograničen pristup transakcijama što rezultira poboljšanom skalabilnošću i privatnošću.

Što se tiče primene programskih jezika, veća podrška za Hyperledger (Go, Java, Javascript), u odnosu na Ethereum (Solidity), je od velikog značaja za razvoj složenih softverskih rešenja iz oblasti upravljanja lancima snabdevanja iz razloga što na tržištu postoji veliki broj obučenih programera iz ovih programskih jezika koji uz manje napora mogu da prihvate razvoj blockchain softverskih rešenja baziranih na Hyperledger-u.

Konačno, Hyperledger ne zahteva primenu kriptovaluta za potvrdu izvršavanja transakcija. Ethereum poseduje vlastitu kriptovalutu Ether kojom se plaća svaka izvršena transakcija. Međutim, Hyperledger i ovde pokazuje visok stepen fleksibilnosti. Zbog visokog stepena programabilnosti, moguće je razviti vlastite tokene za podršku plaćanju obavljenih transakcija.

Prema tome, na osnovu obavljene analize i diskusije, kao platforma za razvoj softverskog rešenja sistema upravljanja lancima snabdevanja, baziranog na blockchain tehnologiji, predlaže se Hyperledger.

PRIKAZ I ANALIZA IZABRANE TEHNOLOGIJE I MODELA SLUČAJA KORIŠĆENJA

Tehnologije koje su privatne i bazirane na dozvolama, kao što je Hyperledger Fabric, tvrde da je moguće napraviti privatnu mrežu sa brzim transakcijama, bržim razvojem pametnih ugovora i određenim pravilima odobrenja za slučaj korišćenja gde je potrebno da grupa pravnih lica i / ili kompanija vrši transakcije na distribuirani, transparentan i automatizovan način. Zato je, a na osnovu prethodnog izlaganja, ovaj rad dobio zaduženje da ispita slučaj korišćenja upravljanja lancem snabdevanja softverskim rešenjem baziranim Hyperledger Fabric mreži.

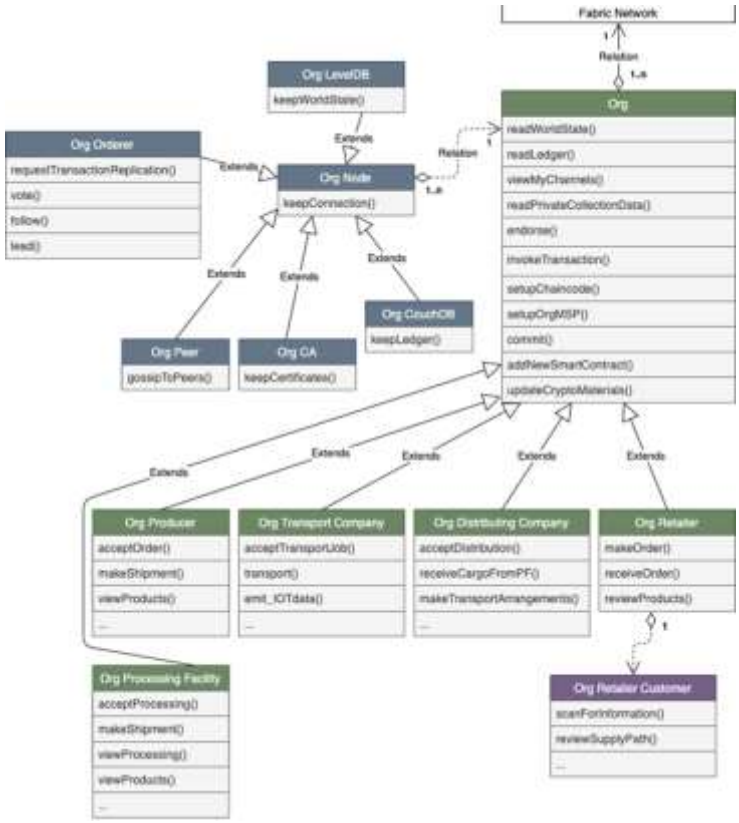
Hyperledger Fabric mreže se sastoje od aktera i čvorova, koji su po mogućnosti maksimalno distribuirani na različitim serverima organizacija (aktera). Pored aktera i čvorova, mreža se sastoji i od distribuiranih pametnih ugovora koji omogućavaju i obezbeđuju (u bezbednosnom kontekstu) kreirane funkcionalnosti i aktivnosti po određenim pravilima slučaja korišćenja - akterima koji su sertifikovani, poznati i prihvaćeni da zajedno učestvuju i rade unutar kreirane i postavljene Hyperledger Fabric mreže.

Dijagram koji služi kao primer entiteta korisnika, mrežnih komponenti i funkcionalnosti je prikazan na slici 3. Sa dijagrama se jasno vidi da je Hyperledger idealan za implementaciju kroz kombinovanje sa nekim objektno-orijentisanim jezikom opšte namene, poput Jave.

MSP (Membership Service Provider) je deo Hyperledger Fabric softverskog interfejsa koji se koristi za identifikovanje učesnika mreže, kao i limitiranje funkcionalnosti čvorovima i organizacijama unutar mreže, poput ACL (access control lists) ili AC (access control) modulima u operativnim sistemima. Potrebno je razlikovati dva tipa MSP-a:

- lokalna MSP komponenta i
- MSP komponenta kanala.

Lokalni MSP je sigurnosni modul koji se može koristiti za određivanje administratora jednog čvora ili aplikacije organizacije koja je u Hyperledger Fabric mreži, odnosno, za određivanje svih administratora jednog čvora ili aplikacije organizacije koja učestvuje u mreži. MSP komponenta kanala se koristi za identifikaciju učesnika jednog kanala i povezivanje tih identiteta sa dozvolama učesnika. MSP kanala će predstavljati javne ključeve ili sertifikate čvorova jedne organizacije. Svaka organizacija zato ima zabeleženu MSP komponentu u konfiguraciji kanala u kojoj funkcionišu i vrše neke transakcije.



Slika 3. Primer komponenti, aktera i njihovih funkcija

U prethodnom izlaganju je dosta bilo govora o pametnim ugovorima i načinima njihove implementacije. U Hyperledger Fabric žargonu govori se o lancu koda (chaincode) ili odomaćenom terminu čejnkod. Pri postavljanju Hyperledger Fabric mreže, pravi se tzv. sistemski lanac koda koji definiše osnovu funkcionalnosti za potrebe određenog slučaja korišćenja kreirane mreže. Pored osnovnog pametnog ugovora, moguće je napraviti i dodatne pametne ugovore kojima se dopunjuju funkcionalnosti mreže.

```
*/
async transportShipment(ctx, orderId) {
}

/**
async receiveShipment(ctx, orderId) {
}

/**
async queryOrder(ctx, orderId) {
}
```
Slika 4. Primer funkcija u pametnom ugovoru

Blockchain mreža je sastavljena od učesnika – aktera koje na osnovu konsenzusa omogućavaju obavljane transakcija u mreži. Svi akteri predstavljaju poslovne entitete, npr. organizacije, udruženja ili kompanije.

U slučaju ovog modela i za slučaj korišćenja lanca snabdevanja ribljim proizvodima, akteri mreže mogu biti sledeći:

- Producer – upravljanja lancem snabdevanja svežih riba, ovaj akter bi bio ribarska kompanija.
- Retailer – prodavnica koja prodaje riblje proizvode.
- Fish Restaurant - restoran koji pravi ponude za ribare.
- Transport – kompanija koji prenosi uhvaćenu ribu od ribara do restorana ili od ribara do fabrike za preradu ribljih proizvoda ili do distributivnog centra.
- Distribution Company – distributivni centar koji u nekom trenutku u lancu snabdevanja kupuje proizvode i prosleđuje ih krajnjim klijentima lanca snabdevanja – ribljem restoranu ili prodavnici.
- Cannery Company – Fish Processing Facility – akter zadužen za neku vrstu prerade ribe u novi proizvod (fabrika neke vrste proizvodnje ili prerade).

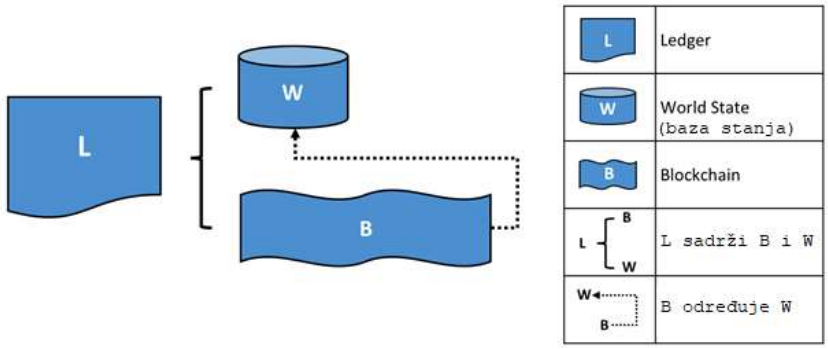
Neki eksterni entiteti koji interaguju ili utiču na rad kompanija i aktera same mreže:

- Regulator – regulatorno telo ili regionalna administrativna organizacija zadužena da obazrivo prati sve transakcije vezane za ribarenje svežih riba, njihov prenos do restorana, fabrike ili radnje i dozvole svih organizacija za poslovni rad na tom području.
- Customer – Gost restorana koji ocenjuje riblja jela i ponude restorana na osnovu iskustva u restoranu i informacija dostupnih iz mreže o istoriji putanje ribe kroz lanac snabdevanja.

Čvorovi (nodes) su mrežne komponente Hyperledger Fabric mreža koje su potrebne za efikasno i sigurno slanje, primanje i obradu svih transakcija unutar mreže. Postoje sledeći čvorovi:

- Peer Node – čvor koji je umrežen sa drugim čvorovima iste funkcije ili namene (tračarenje i prihvatanje informacija P2P).
- LevelDB Node (World State Ledger Node) – čvor koji čuva bazu organizacije gde se skladišti trenutno stanje svih informacija na mreži.
- CouchDB Node (Blockchain Ledger Node) – čvor koji čuva bazu organizacije gde se skladište sve transakcije mreže, uspešne i neuspešne sa svim parametrima koji su prošli kroz mrežu.
- CA (Certificate Authority) Node – čvor koji čuva sertifikate organizacije i njenih zaposlenih koji interaguju sa Hyperledger Fabric mrežom za upravljane lancem snabdevanja (privatne i javne ključeve).
- Ordering Peer Node – čvorovi koji učestvuju u organizaciji transakcija u blok i postavljanju odobrenja za konačno dodavanje bloka u knjige (ledger-e).

Jedan čvor može imati više funkcija, npr. može biti i čvor za potvrđivanje (endorsing) i čvor za izvršavanje i čuvanje – (commiting peer node). Ono što je karakteristično za Hyperledger Fabric mreže jeste postojanje dva tipa baza podataka: baza sa transakcijama (blockchain) i baza sa meta podacima (world state) koja čuva trenutnu vrednost stanja ledger-a (knjige transakcija). Na slici 5 prikazana su dva tipa baza podataka koje se nalaze na čvorovima mreže.



Slika 5. Baze podataka W i B, LevelDB i CouchDB (izvor: hyperledger-fabric.readthedocs.io)

Pre nego što se pokaže predložena struktura mreže (softverskog rešenja) neophodno je dati još par smernica koje se tiču mehanizma konsenzusa i poverljivosti.

Uz pretpostavku da je:

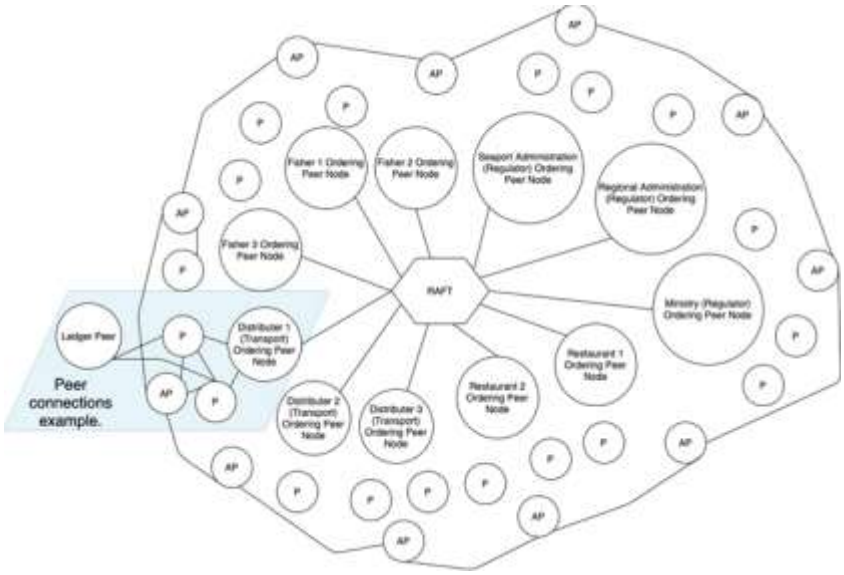
- Predložena aplikacija je portal ka Hyperledger Fabric mreži za podršku lancu snabdevanja.
- Mreža je postavljena sa svim konfiguracijama, kripto materijalima (sertifikatima) i unutar svih organizacija je instaliran pametni ugovor koji sadrži funkcije za različite uloge (role) u mreži.
- Sve komponente su umrežene na postavljenoj mreži.

Politika odobravanja onda izgleda na sledeći način:

- Od aplikacije koja se koristi kao portal za aktere organizacija koje učestvuju u mreži šalje se predlog transakcije - *transaction proposal*. Transakcija je poziv neke funkcije na pametnom ugovoru koji je instaliran.
- Čvorovi koji potvrđuju - *endorsing peers* - proveravaju da li je poziv dobro formiran (standardizovanih ulaznih vrednosti na način koji funkcija zahteva), da li je ta ista transakcija već poslata ranije (odbrana od ponovnih napada – *replay attacks*) i da li je digitalni potpis odgovarajući i validan (provera preko MSP-a).
- Uz pomoć ulaznih parametara pozvane funkcije, čvorovi koji potvrđuju - *endorsing peers* - simuliraju egzekuciju te funkcije nad bazom u trenutnom stanju. Posle toga se vraća nazad odgovor na predlog - *proposal response* - za tu transakciju koji sadrži koje informacije su izmenjene ili dodate u bazi tom istom transakcijom i digitalni potpisi svih čvorova koji potvrđuju. Dakle, u tom trenutku je ta transakcija samo simulirana i nikakve vrednosti nisu stvarno promenjene ili dodate bazama čvorova. Isto uočavamo i za baze podataka svetskog stanja - *world state database* - mreže.
- Aplikacija verifikuje potpise čvorova koji potvrđuju i proveravaju da li su odgovori na predlog - *proposal responses* - od njih isti. Takođe, politika odobravanja mora biti zadovoljena (npr. da li su org1_peer i org4_peer odobrili transakciju).
- Takva transakcija je onda (sa potpisanim odgovorima odobrenja - *endorsement responses* - i informacijama koje su dodate ili izmenjene) emitovana čvorovima servisa za uređivanje, a njihov posao je da sakupljaju sve odobrene transakcije, hronološki ih izlistaju i od njih naprave novi blok.
- Ti blokovi su tada poslati svim čvorovima i transakcije u njima se ponovo proveravaju. Proveravaju se ispunjenja politike odobrenja i trenutna stanja kad je transakcija predložena, kao i u trenutku kada je već u bloku. Transakcije unutar bloka se takođe markiraju, da li su validne ili ne, shodno opisanim pravilnicima za validnost transakcija.
- Zatim sledi rad servisa za uređivanje (ordering service).

Servis za uređivanje je grupa čvorova svih organizacija koji učestvuju u organizaciji svih emitovanih transakcija u jednom periodu. Potrebno je organizovati transakcije u blok po hronološkom redu tj. vremenu kad su otkrivene – emitovane u mreži. U verzijama 1.4.2 i 2.0+ Hyperledger Fabric softvera implementiran je RAFT konsenzus algoritam. U ovom radu neće biti detaljno opisan ovaj algoritam. Ukratko, to je CFT[97] koji je baziran na nasumičnom odabiru glavnog (*leader)* - čvora u određenim intervalima i čvorova sledbenika (*follower*s). Replikacija logova (tj. transakcija u ovom slučaju) je zadatak ovog algoritma. Primer konekcije čvorova, servisa za uređivanje i nekoliko primera aktera za slučaj korišćenja upravljanja lancem snabdevanja ribe i ribljih proizvoda prikazan je sledećom slikom. U središtu primera se nalazi RAFT konsenzus algoritam.

[97] *Crash Fault Tolerant* konsenzus algoritmi su sposobni da održavaju stanje ledgera mreže i u slučaju padova velikog broja čvorova mreže.



Slika 6. Slučaj korišćenja upravljanja lancem snabdevanja ribe i ribljih proizvoda

AP su sidra (anchor peers), čvorovi koji se povezuju sa čvorovima drugih organizacija. Plavom bojom je prikazan primer jedne organizacije i njenih konekcija koje poseduje između svojih čvorova, kao i čvora koji je povezan sa RAFT servisom, kao i sa čvorom koji čuva bazu mreže za tu organizaciju.

Poverljivost informacija unutar same mreže je realizovana kao PDC (Private Data Collections). Ovaj metod se sastoji od sledećih koraka:

- Prvobitno slanje privatnih informacija samo onim organizacijama koje bi trebalo da imaju te informacije.
- Prolazak kroz politiku odobravanja samo za te organizacije – kao dogovor o hešu tih privatnih informacija u transakciji.
- Konačno, organizacije imaju podeljene privatne informacije između sebe, i u tom trenutku može se napraviti javna transakcija na nivou mreže, ali sa hešom poverljivih informacija unutar transakcije koja će biti prosleđena svim čvorovima mreže.

Time je distribuiran heš svim članovima, dok su poverljive informacije, u čitljivom formatu, distribuirane samo kod određenih organizacija i čvorova.

SCENARIO

Sama aplikacija je veoma složena i u jednom radu nije moguće demonstrirati sve elemente implementacije. Opisani su svi najvažniji aspekti analize i dizajna blockchain tehnologije za primeru konkretnog lanca snabdevanja. U nastavku je bitno da se na adekvatan način, grafički pre svega, demonstriraju najbitniji elementi implementacije bazirane na opisanim elementima analize i dizajna.

Za početak je potrebno što bolje integrisati preporuke identifikacije komponenata lanca snabdevanja GS1 standarda (www.gs1yu.org) za svežu hranu u upravljanju lancem snabdevanja:

- Svi komercijalni entiteti treba da imaju GLN (Global Location Number).
- Primer za ribarsku kompaniju koja učestvuje u lancu snabdevanja prikazan je u tabeli 2.

Tabela 2. GS1 identifikatori za ribrasku kompaniju

Komponente	GS1 ID	Dodatni Opis
Geografska lokacija ribarenja.	GLN.	Lokacija gde se lovi riba.
Proizvod i kontejneri na brodu.	GTINs (Global Trade Item Numbers) i SSCCs (Serial Shiping Container Codes).	Za identifikaciju samih riba i kontejnere u koje se smeštaju nakon ulova na brodu.
Emitovanje informacija od strane ribara, broda, kapetana broda.	GTIN i GLN (Global Location Number).	EDI[5] standard je u ovom modelu zamenjen blokčejn mrežom koja rukovodi protok i distribuiranost podataka proizvedenih emitovanjem uređaja ili unosom ribara.

Kako bi proizvod započeo svoj put kroz lanac snabdevanja, akteri prvo prosleđuju ponude jedni drugima kako bi započeli transakcije robe. Jedan ciklus sa svim koracima putovanja proizvoda kroz lanac snabdevanja sledi:

1. Maloprodajna radnja meri svoju listu proizvoda i zahteva kupovinu nove količine. Pravi i šalje upit (za poslovnu saradnju) distribucionom centru.
2. Distribucioni centar pregledava upit i prihvata ga. Potrebna je nabavka proizvoda konzervirane ribe.
3. Distribucioni centar zahteva dobavljanje proizvoda. Pravi i šalje upit centru za proizvodnju konzervirane ribe.
4. Centar za proizvodnju konzervirane ribe pregledava upit i prihvata ga. Potrebna je nabavka ribe za proizvodnju konzerviranih proizvoda.
5. Centar za proizvodnju konzervirane ribe zahteva dobavljanje ribe. Pravi i šalje upit ribarskoj kompaniji.
6. Ribarska kompanija pregledava upit i prihvata ga.
7. U isto vreme, riblji restoran zahteva novu porudžbinu sveže ribe od ribara. Potražnja za ribljim jelima koja se služe mušterijama - postoji.
8. Riblji restoran šalje upit ribarskoj kompaniji.
9. Ribarska kompanija pregledava upit i prihvata ga.
10. Pre prihvatanje ponude, ribarska kompanija ima postavljene svoje proizvode kao ponude za kupovinu, za koje se vezuju ponude ribljeg restorana ili centra za proizvodnju konzervirane ribe. Za svaki proizvod ili seriju proizvoda, ponudu i količinu proizvoda - regulatorno telo proverava proizvod i daje dozvolu za prodaju određenog proizvoda ili serije proizvoda. Dokumenti o potvrdi validnosti proizvoda i ponude se od ribarske kompanije i od centra za proizvodnju konzervirane ribe prosleđuju dalje u lancu snabdevanja.
11. Sve ponude imaju vremensko ograničenje za isporuku kao i dodatne IOT senzorske limite vezane za transport robe od aktera A do aktera B. Ti IOT senzorski limiti mogu biti ograničenja za temperaturu i učestalost GPS emitovanja kontejnera (koji čuvaju i sadrže proizvode) koji su u tranzitu.
12. Ribarska kompanija stvara izvorni resurs i od tog proizvoda zapravo počinje put kroz lanac snabdevanja u drugom smeru, ka maloprodajnoj radnji ili ka ribljem restoranu.
13. Ribarska kompanija šalje ponudu transportnoj kompaniji 1 za posao prenošenja kontejnera ulovljene ribe do ribljeg restorana.
14. Transportna kompanija 1 pregledava ponudu i prihvata je. Riblji restoran dobija informacije o transportu emitovanjem kroz mrežu i očekuje transport da stigne od strane transportne kompanije 1.
15. Transportna kompanija 1 emituje informacije svih IOT senzora na kontejnerima tokom transporta i završava prenos robe kad stigne do ribljeg restorana.
16. Riblji restoran potvrđuje da je roba stigla i proverava stanje kontejnera i količinu robe. Transakcija između ribljeg restorana i ribarske kompanije je uspešno kompletirana.
17. Gosti restorana mogu imati opciju da skeniranjem QR koda na računu naručenog jela

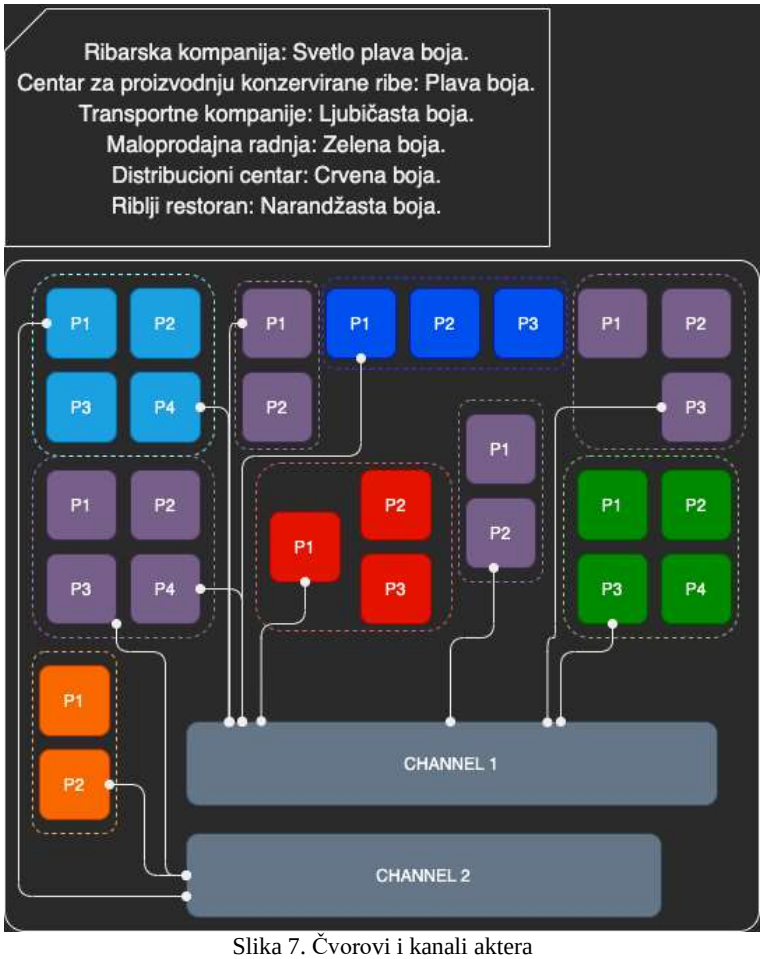
pregledaju put ribe u jelu koju su dobili od ribara do restorana.

18. Pored toga, ribarska kompanija šalje ponudu transportnoj kompaniji 2 za posao prenošenja kontejnera ulovljene ribe do centra za proizvodnju konzervirane ribe.
19. Transportna kompanija 2 pregledava ponudu i prihvata je. Centar za proizvodnju konzervirane ribe dobija informacije o transportu emitovanjem kroz mrežu i očekuje transport da stigne od strane transportne kompanije 2.
20. Transportna kompanija 2 emituje informacije svih IOT senzora na kontejnerima tokom transporta i završava prenos robe kad stigne do centra za proizvodnju konzervirane ribe.
21. Centar za proizvodnju konzervirane ribe potvrđuje da je roba stigla i proverava stanje kontejnera i količinu robe. Transakcija između centra za proizvodnju konzervirane ribe i ribarske kompanije je uspešno kompletirana.
22. Centar za proizvodnju konzervirane ribe šalje ponudu transportnoj kompaniji 3 za posao prenošenja kontejnera ulovljene ribe do distribucionog centra.
23. Transportna kompanija 3 pregledava ponudu i prihvata je. Riblji restoran dobija informacije o transportu emitovanjem kroz mrežu i očekuje transport da stigne od strane transportne kompanije 3.
24. Transportna kompanija 3 emituje informacije svih IOT senzora na kontejnerima tokom transporta i završava prenos robe kad stigne do distribucionog centra.
25. Distribucioni centar potvrđuje da je roba stigla i proverava stanje kontejnera i količinu robe. Transakcija između centra za proizvodnju konzervirane ribe i distribucionog centra je uspešno kompletirana.
26. Distribucioni centar šalje ponudu transportnoj kompaniji 4 za posao prenošenja kontejnera ulovljene ribe do maloprodajne radnje.
27. Transportna kompanija 4 pregledava ponudu i prihvata je. Maloprodajna radnja dobija informacije o transportu emitovanjem kroz mrežu i očekuje transport da stigne od strane transportne kompanije 4.
28. Transportna kompanija 4 emituje informacije svih IOT senzora na kontejnerima tokom transporta i završava prenos robe kad stigne do maloprodajne radnje.
29. Maloprodajna radnja potvrđuje da je roba stigla i proverava stanje kontejnera i količinu robe. Transakcija između distribucionog centra i maloprodajne radnje je uspešno kompletirana.
30. Jedan ciklus lanca snabdevanja do ribljeg restorana i do maloprodajne radnje je završen.

Slede pretpostavke i ograničenja scenarija:

- Ceo lanac snabdevanja je smešten u jednoj administrativnoj regiji ili državi.
- IOT senzori za emitovanje informacija tokom transporta robe smatraju se proverenim od strane treće strane ili kompanije zadužene za tu svrhu, a koja nije u mreži modela.
- Regulatorno telo je eksterni akter koji mora da verifikuje i da izda potvrdu o verifikaciji napravljenih proizvoda kod aktera – ribarska kompanija i centar za proizvodnju konzervirane ribe - jer oni nalaze (ribare) ili prave nove proizvode u sistemu.
- U slučaju povraćaja robe, u ovom slučaju ribe ili ribljih proivoda, aktera koji primaju robu od nekog prethodnog aktera u sistemu, pretpostavlja se da je inspekcija od strane nezavisnog ili sudskog veštaka već obavljena, posle prijave da je roba ili kontejner koji je pakovanje robe kontaminiran ili oštećen. Dakle, u scenariju neće biti prikazan proces povraćaja robe.
- Postoje vrste čvorova za povezivanje sa drugim organizacijama, izvršavanje i čuvanje blokova, odobravanje predloga transakcija i za servis za uređivanje (anchor, commiting i endorsing, ordering čvorovi). Vrste nisu označene pojedinačno, ali svaka organizacija ima bar jedan čvor za svaki tip čvora.
- Svi čvorovi, kanali, pametni ugovori su podignuti i instalirani na mreži. Pametni ugovori su napisani Java programskim jezikom na Hyperledger Fabric. Funkcije aktera su funkcije implementirane u pametnim ugovorima.
- Baze podataka organizacija su one koje su preporučene od strane Hyperledger Fabric projekta, LevelDB i CouchDB.

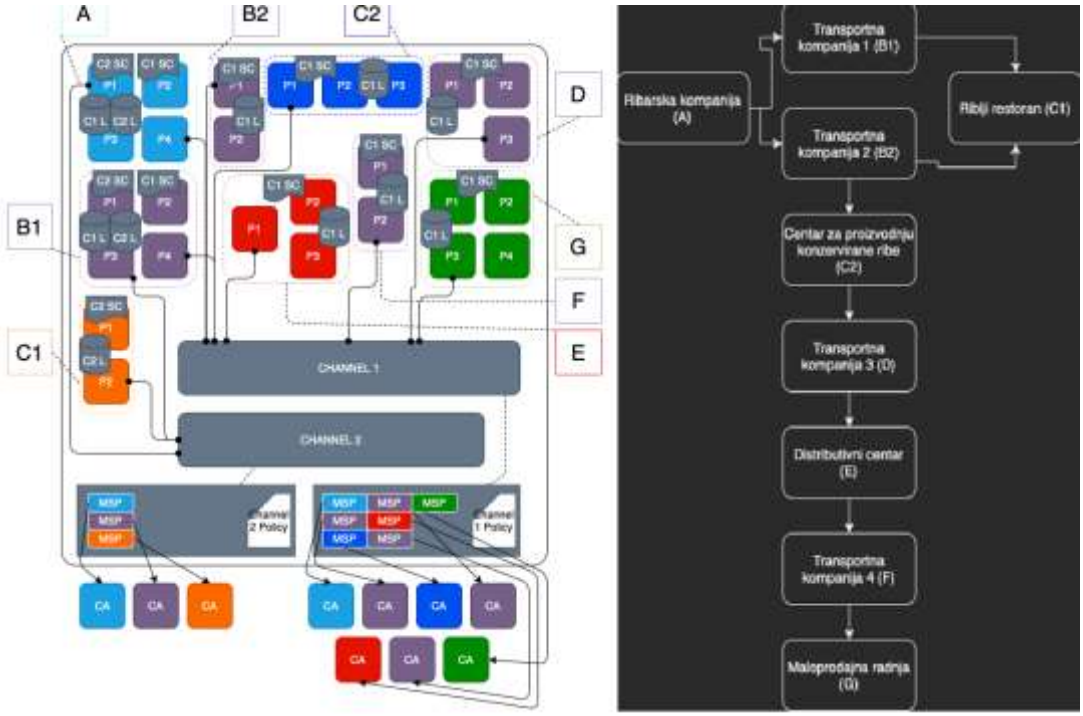
Akteri u mreži, raspoređeni po kanalima, prikazani su slikom 7:



Slika 7. Čvorovi i kanali aktera

Slika 7. je odličan osnov za kompletiranje modela implementacije blockchain mreže za podršku procesu lanca snabdevanja. Dodavanjem komponenata: MSP komponente aktera, CA komponente aktera, raspored pametnih ugovora, raspored baza kanala, kao i odgovarajućih oznaka za svakog aktera obuhvaćenog scenarijom, dobija se konačna verzija modela nad kojim se vrši implementacija blockchain mreže (desni grafikon na slici 8).

Konačno, izlaganje se završava demonstracijom tokova transakcija koje se odigravaju unutra opisane blockchain mreže. Tokovi transakcija su opisani desnim grafikonom na slici 8.



Slika 8. Konačan model i tokovi transakcija

ZAKLJUČAK

Rad se fokusirao na analizu i diskusiju izbora optimalne blockchain tehnologije za savremeni način skladištenja, obrade i distribucije podataka u informacionim sistemima za podršku lancima snabdevanja.

Poređena su dva pristupa:

- Ethereum;
- Hyperledger, odnosno njegova distribucija Hyperledger Fabric.

Izbor je baziran na specifičnim kriterijumima blockchain tehnologije:

- Svrha;
- Poverljivost;
- Vrsta mreže;
- Podrška mehanizmima konsenzusa;
- Podrška u formi programskih jezika;
- Podrška za kriptovalute.

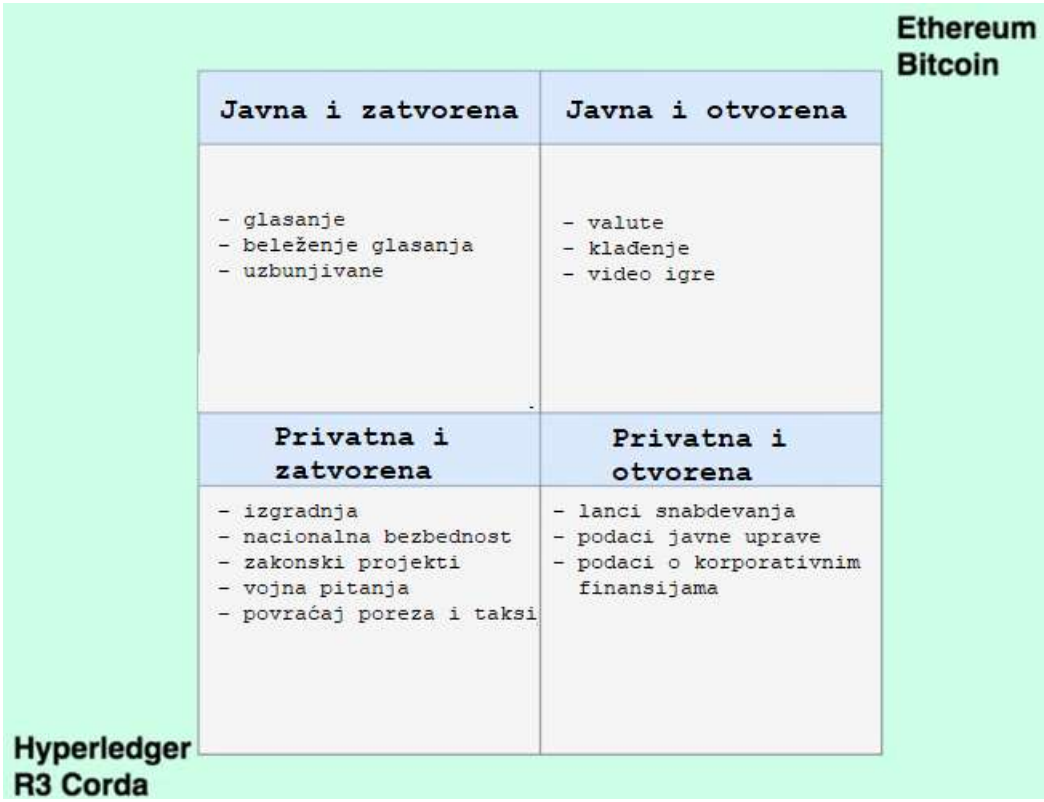
Po svim kriterijumima, osim podrške za kriptovalute, iako je zbog visoke fleksibilnosti moguće uvesti vlastite tokene plaćanja, kao optimalno rešenje za primenu blockchain tehnologije u softverskom rešenju za podršku lancu snabdevanja, identifikovan je Hyperledger Fabric i oko njega je vođena dalja analiza i diskusija. Kao poseban deo rada ističe se studija slučaja na uvođenju blockchain tehnologije, bazirane na Hyperledger Fabric platformi, za podršku lancu snabdevanja ribljim proizvodima. Detaljno su opisani:

- Scenario upotrebe;
- Akteri i kanali u mreži;
- Način izbora i primene algoritma mehanizma konsenzusa;
- Topologija mreže;
- Tokovi transakcija unutar mreže.

Ono što nije prikazano u ovom radu, a tiče se konačne definicije modela jesu standardni dijagrami koji su obavezni, podrazumevani i dobro poznati i prisutni u ogromnom broju radova, kao i projektne dokumentacije, poput sekvencijalnih dijagrama za različite scenarije primene unutar ovakvog informacionog sistema.

Sigurno je da ovakav pristup ima dosta prostora za unapređenje u smislu efikasnijeg i efektivnijeg konačnog softverskog rešenja. Radi se o veoma mladoj tehnologiji i usled nedostatka adekvatne obuke, kao i literature, istraživači i programeri su u velikoj meri prepušteni eksperimentisanju i isprobavanju različitih scenarija. Međutim, radi se o izuzetno rastućoj tehnologiji koja će svakako doneti brojne benefite svim korisnicima i učesnicima blockchain mreže, a ključni je svakako podizanje poverenja između svih učesnika mreže.

Konačno, rad koji se bavio poređenjem i izborom različitih blockchain tehnologija kao zaključnu ilustraciju prilaže sliku kojom se ilustruje u kojim oblastima određene tehnologije daju bolje rezultate.



Slika 9. Oblasti optimalne primene različitih blockchain tehnologija

LITERATURA

Nakamoto, S. (2009) Bitcoin: A peer-to-peer electronic cash system. *Whitepaper*

Chen W, Xu Z, Shi S, Zhao Y, Zhao J. (2018). A Survey of Blockchain Applications in Different Domains, *International Conference on Blockchain Technology and Applications (ICBTA) 2018*, December 10–12, 2018, Xi'an, China

Bayon, P, S. (2019). Key Legal Issues Surrounding Smart Contract Applications, *SSRN Electronic Journal 9(1):63-91*

Tribis Y, El Bouchti A, Bouayad H. (2018). Supply Chain Management based on Blockchain: A Systematic Mapping Study, *MATEC Web of Conferences 200(2):00020*

https://www.edureka.co/blog/hyperledger-vs-ethereum/ (vreme pristupa 30. 07. 2020. u 23:15)

Kosba A, Miller A, Shi E, Wen Z, Papamathou C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, *2016 IEEE Symposium on Security and Privacy (SP)*

Idelberger F., Governatori G., Riveret R., Sartor G. (2016) Evaluation of Logic-Based Smart Contracts for Blockchain Systems, *International Symposium on Rules and Rule Markup Languages for the Semantic Web RuleML 2016: Rule Technologies. Research, Tools, and Applications pp 167-183*

Alhabry M, Van Morsel A. (2017). Blockchain-based Smart Contracts: A Systematic Mapping Study, *Fourth International Conference on Computer Science and Information Technology (CSIT-2017)*

Metcalfe W. (2020). Ethereum, Smart Contracts, DApps, *In book: Blockchain and Crypt Currency*, *DOI: 10.1007/978-981-15-3376-1_5*

https://www.abra.com/resources/worlds-computer/ (vreme pristupa 31. 07. 2020. u 16:15)

Sarkar P. (2020). A New Blockchain Proposal Supporting Multi-Stage Proof-of-Work, *https://eprint.iacr.org/2019/162.pdf*

https://hyperledger-fabric.readthedocs.io/en/release-2.0/ledger/ledger.html#what-is-a-ledger (vreme pristupa 01. 08. 2020. u 09:15)

http://www.gs1yu.org/standards.html (vreme pristupa 05. 08. 2020. u 16:15)

BLOCKCHAIN TECHNOLOGY CHOICE FOR THE IMPLEMENTATION OF THE SOFTWARE SOLUTION IN A SPECIFIC AREA OF SERVICES OR INDUSTRY

Vladimir Milićević, Igor Franc, Andrija Đurić

Belgrade Metropolitan University, Tadeuša Košćuška 63, 11 158, Belgrade, Serbia,
vladimir.milicevic@metropolitan.ac.rs

ABSTRACT

In the modern software industry, which is in constant expansion, the problem of trust between different users of the software solution is becoming increasingly dominant. End users want to be completely sure that the product or service is fully compliant with their requirements and that the quality does not deviate from the selected or ordered product or service. Manufacturers or service providers, on the other hand, want to have complete information about the quality of raw materials or infrastructure they provide in order to create products and services, which should be provided by the appropriate supplier. All participants in the software solution (actors) as an imperative have the security of their own data that is stored, processed and exchanged within such software system.

The aim of this paper is to demonstrate the application of an innovative approach in the storage, processing and exchange of information using blockchain technology with a case study on the supply chain. There are different approaches and in the first step the corresponding ones will be compared: Ethereum and Hyperledger Fabric blockchain network / platform. After selecting the appropriate technology, the work will focus on examining the potential security solutions that blockchain technology provides for the needs of the use case. This means that it is first necessary to explain the specific concepts of blockchain technology, then make a use case model, describe it in detail and deepen it to an adequate extent, and finally test some hypotheses related to improving transparency, information integrity, maintaining network security, maintaining effective initiatives for participation and defense against bad motivations of all actors within the system.

Keywords: blockchain, software system, platform, trust, actors.