Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.738.5:339
DOI: https://doi.org/10.24867/31BE03Stamenkovic

SKLADIŠTENJE I RAZMENA ZDRAVSTVENIH PODATAKA PRIMENOM BLOCKCHAIN TEHNOLOGIJE

STORAGE AND EXCHANGE OF HEALTH DATA USING BLOCKCHAIN TECHNOLOGY

Lea Stamenković, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Rad istražuje primenu blockchain tehnologije u zdravstvu, sa posebnim osvrtom na razmenu i sigurnost podataka o pacijentima. U radu su analizirani problemi sa kojima se suočava zdravstvena industrija, predstavljena su dosadašnja rešenja i objašnjena ključna terminologija. Istaknute su prednosti koje blockchain donosi u ovoj oblasti, uključujući decentralizaciju i sigurnost. Tehnologija blockchain-a je detaljno razmatrana kroz opis njenih elemenata, načina funkcionisanja, kao i izazova u primeni. Rad obuhvata i opis implementacije rešenja zasnovanog na blockchain-u, koristeći IPFS za skladištenje podataka, Spring Boot za back-end, te Angular za front-end aplikaciju.*

Ključne reči: *Medicina, EHR, Blockchain, Hyperledger Fabric, razmena zdravstvenih podataka*

Abstract – *The paper explores the application of blockchain technology in healthcare, with a focus on the exchange and security of patient data. It analyzes the challenges faced by the healthcare industry, presents existing solutions, and explains key terminology. The advantages that blockchain brings to this field, including decentralization and security, are highlighted. The technology is thoroughly examined through a description of its elements, functioning, and the challenges of its implementation. The paper also includes a description of a blockchain-based solution, using IPFS for data storage, Spring Boot for the back-end, and Angular for the front-end application.*

Keywords: *Medicine, electronic health records (EHR), blockchain, Hyperledger Fabric, health data storage and exchange*

1. UVOD

Ključni deo svake medicinske ustanove čini medicinska dokumentacija. Mnoge organizacije, među kojima je i Svetska Zdravstvena Organizacija (WHO), decenijama u nazad rade na sistematizaciji samog procesa kreiranja medicinskih dokumenata, u cilju smanjenja broja nedostajućih i netačnih podataka u njima. Mogućnost da zdravstveni radnici digitalno čuvaju podatke o pacijentu uz obezbeđenu sigurnost tih podataka u mnogome je doprinela povećanju efikasnosti i smanjenju troškova. U proteklim decenijama, EHR sistemi su postali ključni za savremenu zdravstvenu zaštitu, ali uprkos njihovoj širokoj upotrebi, određeni izazovi i dalje postoje. Interoperabilnost se navodi kao jedan od značajnih problema EHR sistema koji su trenutno u upotrebi [1]. Takođe, skorašnje studije pokazuju da je broj povreda u značajnom porastu u proteklih par godina, gde se ističu hakovanje, IT incidenti i neovlašćeni pristup kao najčešći načini povrede podataka [2]. Povrede podataka naglašavaju rastuću ranjivost osetljivih informacija, ali takođe pokazuju značajne bezbednosne izazove i izazove privatnosti EHR sistema. Za rešavanje pomenutih problema, sve više pažnje privlači blockchain tehnologija [3]. Zbog svoje pouzdanosti i interoperabilnosti, blockchain pruža bezbednu infrastrukturu za deljenje EHR podataka između ovlašćenih strana. Uz pomoć pametnih ugovora i mehanizama konsenzusa između učesnika u mreži, blockchain omogućuje potpunu kontrolu nad pristupom podacima. Time zasigurno obezbeđuje povećanu sigurnost i privatnost kao osnovnu prednost primene. Uklanjanjem centralizovanih odluka i oslanjanjem na kriptografske algoritme, blockchain značajno smanjuje rizik od neovlašćenog pristupa i povrede podataka. Dodatno, blockchain možemo posmatrati i kao okvir (framework), koji omogućava nesmetanu razmenu podataka između različitih entiteta u zdravstvu, nezavisno od sistema koje oni trenutno koriste [4].

2. KRIPTOGRAFIJA

Kriptografija predstavlja metod zaštite podataka putem kodiranja, kako bi se sprečio pristup neovlašćenim licima. Ona igra ključnu ulogu u blockchain, gde obezbeđuje sigurnost transakcija, autentifikaciju korisnika i integritet podataka. Blockchain koristi kriptografske heševe za povezivanje blokova, čime se osigurava da podaci u lancu ne mogu biti promenjeni bez otkrivanja.

2. BLOCKCHAIN

Blockchain [5] je distribuirana baza podataka koja čuva informacije o transakcijama među entitetima bez centralnog autoriteta. Održavaju je članovi mreže, a svaka nova transakcija se vezuje za prethodnu, čime nastaje lanac blokova. Zahvaljujući kriptografskim heš funkcijama, podaci se ne mogu menjati bez saglasnosti većine čvorova, čime se obezbeđuje integritet i

---

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

nepromenljivost podataka. Mreža je peer-to-peer, što znači da su svi čvorovi ravnopravni i mogu direktno komunicirati, čime se povećava otpornost na kvarove. Iako se podaci mogu dodavati, njihovo menjanje zahteva velike resurse i saglasnost više od 50% čvorova. U suštini, blockchain funkcioniše kao sigurni distribuirani registar koji omogućava transparentnost i poverenje među korisnicima.

3. HYPERLEDGER FABRIC

Hyperledger Fabric (HLF) [6] je modularni blockchain radni okvir koji omogućava razvoj rešenja i aplikacija zasnovanih na blockchain tehnologiji uz korišćenje modularnih komponenata. Radi implementacije ovakve arhitekture, HLF sadrži modularne blokove: ordering servis, Membership service provajder, peer-to-peer protokol za prosleđivanje informacija, pametne ugovore, glavnu knjigu. **Glavnu knjigu** u HLF blockchain-u čine stanje i blockchain. Stanje (world state) predstavlja bazu podataka koja čuva trenutne vrednosti stanja na blockchain-u. Blockchain je zapis svih transakcija koje su dovele do trenutnog stanja. Ove transakcije su organizovane u blokove povezane u lanac. Za razliku od stanja, podaci u blockchain-u se ne mogu naknadno menjati. **Pametan ugovor** je kod – koji poziva aplikacija klijenta izvan mreže blockchain-a – koji upravlja pristupom i izmenama skupa ključ-vrednost u glavnoj knjizi (tj. world state). U HLF, pametni ugovori nazivaju se chaincode. Chaincode pametnog ugovora instalira se na čvorove i inicijalizuje na jedan ili više kanala. **Ordering servis** predstavlja skup čvorova koji slažu transakcije u blok. Funkcioniše nezavisno od procesa čvorova i slaže transakcije na osnovu principa "prvi dođe, prvi uslužen" za sve kanale na mreži. Ordering servis je zajednički za celu mrežu i sadrži kriptografske identitete povezane sa svakim članom. **MSP** je zadužen za autentifikuju, autorizuju i upravljaju identitetima na blockchain mreži, ali i autentifikuju i autorizuju i blockchain operacije. On predstavlja apstraktnu komponentu sistema koji pruža akreditive klijentima i čvorovima kako bi učestvovali u HLF mreži. Klijenti koriste ove akreditive za autentifikaciju svojih transakcija, a čvorovi koriste ove akreditive za autentifikaciju rezultata obrade transakcija (*endorsement*).

4. BLOCKCHAIN I ZDRAVSTVO

Zdravstvena industrija suočava se sa nizom specifičnih potreba, naročito u pogledu sigurnosti, privatnosti podataka i efikasnog upravljanja informacijama. Osetljivost medicinskih podataka nameće stroge regulatorne zahteve, što značajno otežava njihovu razmenu između različitih aktera u zdravstvu. Pored toga, trenutni sistemi za upravljanje medicinskim podacima često su decentralizovani i fragmentirani, što dodatno komplikuje efikasan protok informacija.

Zdravstveni sistemi imaju potrebu za tehnologijom koja može povezati različite delove industrije, omogućiti verifikaciju podataka, ali i garantovati integritet i nepovredivost informacija. Blockchain nudi infrastrukturnu osnovu koja može podržati sve ove zahteve, pružajući okvir u kojem su informacije lako dostupne ovlašćenim korisnicima, a istovremeno zaštićene od neovlašćenih pristupa ili manipulacija. Primena blockchain tehnologije u zdravstvu polako postaje sve veća. Prema skorašnjim predviđanjima, globalno tržište blockchain-a u zdravstvu očekuje skok od 23-60%, do 2030. godine. Ovaj rast najlakše je objasniti razvojem blockchain tehnologije kroz različite generacije, gde se za generaciju X ističe korišćenje blockchain-a u svakodnevnom životu kroz veštačku inteligenciju.

3.1 Relevantni radovi

MedRec [7] je blockchain sistem za upravljanje medicinskim podacima, razvijen za poboljšanje sigurnosti i kontrole pristupa zdravstvenim informacijama koristeći Ethereum mrežu. Sistem omogućava pacijentima da kontrolišu ko ima pristup njihovim podacima putem pametnih ugovora na blockchain-u. Ovi ugovori omogućavaju odobravanje ili odbijanje pristupa zdravstvenim radnicima i institucijama. MedRec implementira tri vrste ugovora: Ugovor o Registraciji (RC), koji preslika identifikacione stringove na Ethereum adrese i reguliše registraciju novih identiteta; Ugovor o Odnosima Pacijent-Pružalac (PPR), koji upravlja medicinskim zapisima između pacijenata i pružalaca usluga; i Ugovor o Rezimeu (SC), koji sadrži istoriju medicinskih zapisa. Sistem se integriše sa postojećom infrastrukturom za elektronske medicinske zapise (EMR) kroz četiri softverske komponente: Backend Biblioteku, Ethereum Klijenta, Čuvara Baze Podataka i EMR Menadžera. MedRec koristi Proof of Work (PoW) kao osnovni konsenzusni algoritam, ali uvodi dodatne modele motivacije za rudarstvo specifične za zdravstveni sektor.

UniRec (Unified Medical Records) [8] sistem funkcioniše kao privatna peer-to-peer (P2P) mreža koju dele različite zdravstvene organizacije. U ovoj mreži, blockchain Ethereum održava zajedničku istoriju svakog EHR-a, dok se medicinski podaci razmenjuju između institucija preko IPFS-a. UniRec koristi Node.js za upravljanje blockchain-om i šifrovanje sadržaja, dok pametni ugovori omogućavaju kontrolu pristupa.

MedicalChain [9] je platforma koja omogućava pacijentima da kontrolišu pristup svojim podacima putem pametnih ugovora, dok se transakcije beleže na blockchain-u. MedicalChain ima sistem plaćanja koristeći tokene (MedTokens), koje pacijenti mogu koristiti za različite usluge. Model se sastoji od dvostruke blockchain strukture, pri čemu jedna kontroliše pristup zdravstvenim zapisima, a druga služi kao osnova za aplikacije i usluge platforme.

4. MODEL SISTEMA

4.1. Arhitektura sistema

Sistem je dizajniran korišćenjem savremenih tehnologija, uključujući Angular za front-end, Spring za back-end, Hyperledger Fabric za blockchain infrastrukturu i IPFS za skladištenje datoteka. Ova arhitektura omogućava i sigurno i efikasno upravljanje podacima pacijenata.

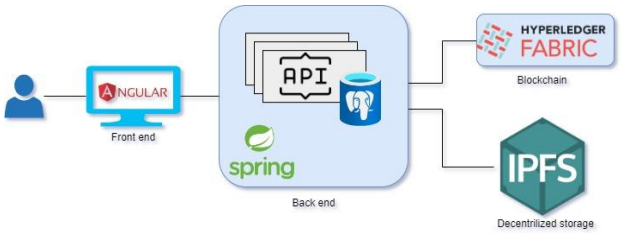
Angular aplikacija omogućava korisnicima interakciju putem web pretraživača, s intuitivnim korisničkim interfejsom za pregled i ažuriranje pacijentskih kartona. Koristi REST API-je za komunikaciju sa Spring back-end aplikacijom.

Spring back-end upravlja poslovnom logikom, autentifikacijom i autorizacijom, kao i obradom podataka. Uključuje API-je za interakciju sa Hyperledger Fabric i upravljanje IPFS-om za skladištenje dokumenata, kao i REST API za komunikaciju sa front-end-om.

Hyperledger Fabric pruža privatni blockchain okvir za sigurno upravljanje podacima. Pametni ugovori upravljaju poslovnim pravilima i verifikacijom transakcija, osiguravajući nepromenljivost i sigurnost podataka.

IPFS omogućava distribuirano skladištenje velikih datoteka povezanih sa pacijentskim kartonima. Dokumenti se skladište na IPFS-u, dok se veze do njih čuvaju na blockchain-u, olakšavajući preuzimanje i deljenje uz očuvanje integriteta.

Arhitektura sistema prikazana je na slici 1.



Slika 1. *Arhitektura rešenja*

4.2 Funkcionalnosti sistema

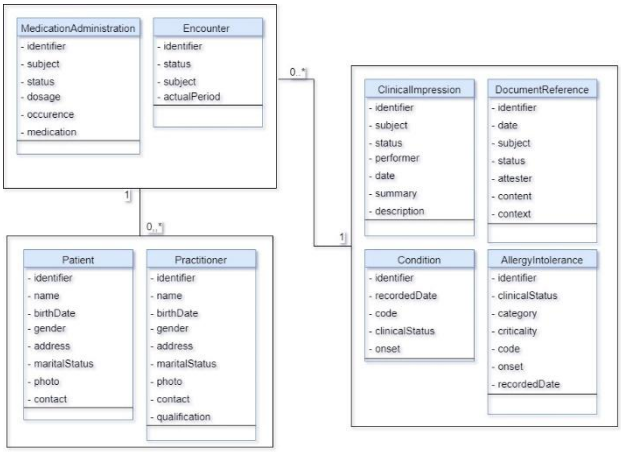
U sistemu su identifikovani sledeći akteri: lekari, pacijenti i administratori. Lekari koriste sistem za pregled pacijenta, pristup i ažuriranje pacijentskih kartona. Pacijenti imaju mogućnost da pregledaju svoje kartone, ažuriraju osnovne podatke i pregledaju logove pristupa svom kartonu. Administratori su odgovorni za upravljanje korisničkim nalozima. Sva tri tipa korisnika imaju mogućnost da menjaju podatke koji se eksplicitno tiču aplikacije (imejl, lozinka,..). Takođe, prepoznajemo i neregistrovanog pacijenta kao deo sistema, kom je omogućeno da se registruje, čime će, ukoliko njegov karton ne postoji već u sistemu, isti biti i kreiran. Ukoliko neregistrovan pacijent već ima postojeći karton u sistemu, ali nije deo aplikacije, kreiraće se novi nalog u okviru aplikacije koji će biti povezan sa njegovim postojećim kartonom.

4.3. Model podataka

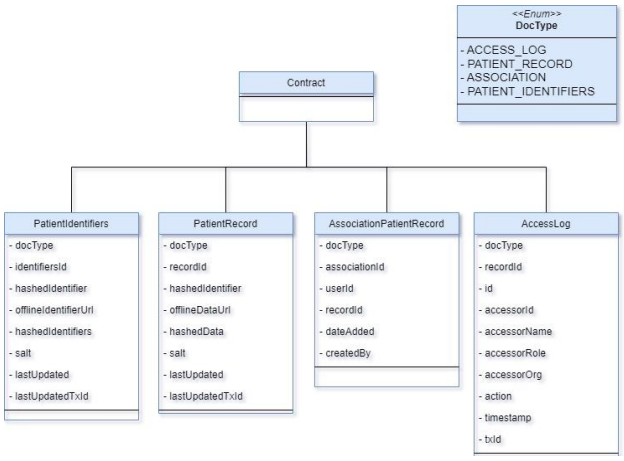
Back-end Spring aplikacija čuva informacije o korisniku, sa atributima koji ga definišu. Svaki korisnik ima podatke potrebne za autentifikaciju (email, password) i osnovne informacije (ime, prezime, imagePath).

Podaci o pacijentskom kartonu čuvaju se van blockchain mreže. Oni predstavljaju skup HAPI FHIR [10] resursa. Dijagram koji prikazuje polja off-chain podataka prikazan je na slici 2.

Podaci na mreži, prikazani na slici 3, služe kako bi se odredila prava pristupa podacima, povezao korisnik platforme sa njegovim kartonom, kao i da bi se proverio integritet podataka sačuvanih u off-line bazi. Model AssociationPatientRecord, omogućava povezivanje objekta PatientIdentifiers i PatientRecord. Ovakva implementacija omogućava da se na osnovu identifikatora kojeg korisnik koristi u zdravstvenim ustanovama poveže karton pacijenta sa već postojećim u sistemu. Ove informacije nalaze se unutar PatientRecord. Međutim dalje u komunikaciji se ne koristi njegov identifikator, već identifikator iz same aplikacije, što se čuva u PatientIdentfiers. Ovaj objekat skuplja sve identifikatore jednog korisnika koje on ima potencijalno u više zdravstvenih institucija. Model AccessLog skladišti sve pristupe pacijentskim kartonima.



Slika 2. *Model podataka u bazi van mreže*



Slika 3. *Model podataka unutar mreže*

5. IMPLEMENTACIJA

5.1 FHIR

Jedan od zahteva zadatka bio je i omogućiti nesmetanu razmenu pacijentskih kartona između različitih institucija. Da bi ovo bilo moguće, korišćen je standard FHIR i njegova Java implementacija HAPI FHIR *(Health API Fast Healthcare Interoperability Resources*). U ovom projektu korištena je samo radi strukturiranja podataka, u skladu sa standardom koji je dobro poznat u zdravstvu.

5.2 IPFS

IPFS (*InterPlanetary File System*) je distribuirani fajl sistem zasnovan na peer-to-peer mreži. Adresiranje u ovom fajl sistemu je zamenjeno adresiranjem zasnovanim na sadržaju. Drugim rečima, za pretragu nekih podataka potreban je njihov heš, a ne adresa na kojoj se nalaze. Kada se fajl pošalje na IPFS radi skladištenja, generiše se jedinstveni heš za taj fajl. Stoga, za pronalaženje tog fajla, potrebno je pretražiti njegov heš. Zbog decentralizacije, očuvanja privatnosti i nepromenljivosti podataka na IPFS-u, ovaj fajl sistem je korišten u projektu kao off-line baza, na kojoj su skladišteni pacijentski kartoni.

5.3 Blockchain

Blockchain mreža ovog projekta razvijena je korišćenjem Hyperledger Fabric (HLF), koji implementira privatnu permissioned blockchain mrežu. Ovaj tip mreže je izuzetno pogodan za primenu u zdravstvu, gde je ključno ograničiti pristup informacijama samo na entitete koji pripadaju zdravstvenim institucijama ili su njihovi korisnici. Pristup mreži zahteva posedovanje sertifikata koji dokazuje identitet korisnika, a upravljanje identitetima je u potpunosti podržano unutar sistema.

U implementaciji je korišćena testna mreža, detaljno opisana u dokumentaciji Hyperledger Fabric-a [6], koja predviđa postojanje dve organizacije uz mogućnost uključivanja treće. Između ovih organizacija kreiran je kanal koji omogućava sigurnu razmenu informacija. Mreža je takođe postavljena uz korišćenje infrastrukture ključeva, što znači da svaka organizacija ima svoj CA (Certificate Authority) koji potpisuje sertifikate koje izdaju te organizacije.

Postizanje dogovora u HLF mreži zavisi od politike odobravanja i pametnog ugovora. Politika odobravanja definiše ko ima pravo da odobri ili odbije određene radnje. U testnoj mreži, politika odobravanja konfigurisana je tako da zahteva odobrenje od bilo kog čvora kanala. Pametan ugovor se instalira na kanal, i svaki čvor organizacije koja je deo kanala. Pametan ugovor omogućava granuliranu kontrolu pristupa resursima na mreži, i enkapsulira poslovnu logiku. U ovom slučaju, pametan ugovor vrši provere uloge korisnika sistema i na osnovu tih provera odobrava određene akcije nad podacima, čime se obezbeđuje da samo ovlašćeni korisnici mogu izvršavati kritične operacije. Primer funkcije pametnog ugovora u kojoj se dobavlja pacijentski karton prikazan je u listingu 1.

```
async GetPatientRecord(ctx, hashedUserId,time) {
   let role = await Util.GetUserRole(ctx);
   if(role !== 'ROLE_PRACTITIONER'){
      throw new Error('unauthorized access to
patient record!'); }
   let association = await
AssociationPatientRecordChaincode.GetAssociation
(ctx, hashedUserId);
   if(!association){
      throw new Error('Invalid patient id.'); }
   let patientRecord = await
PatientRecordChaincode.GetPatientRecord(ctx,
association.recordId);
   await AccessLogChaincode.AddAccessLog(ctx,
association.recordId, time, Action.VIEW);
   return JSON.stringify(patientRecord); }
```

Listing 1. – *Primer funkcije pametnog ugovora*

6. ZAKLJUČAK

U ovoj studiji istraživana je primena blockchain tehnologije u razmeni i čuvanju pacijentskih kartona, s fokusom na koristi i izazove u zdravstvu.

Blockchain nudi značajne prednosti u sigurnosti, transparentnosti i integritetu podataka. Elektronski zdravstveni zapisi (EHR) su ključni za efikasno upravljanje informacijama, a korišćenje blockchain-a omogućava sigurno čuvanje i razmenu podataka među različitim entitetima u zdravstvenom sistemu.

Tehnologija donosi revoluciju u čuvanju i razmeni podataka, nudeći poboljšanja u bezbednosti i kontroli pristupa. U budućnosti, moguća su dalja unapređenja poput kreiranja više kanala unutar blockchain mreže sa različitim pametnim ugovorima, kao i povećane kontrole pristupa koju definišu sami pacijenti, što bi poboljšalo privatnost i sigurnost podataka. Uvođenje uređaja za unos informacija u realnom vremenu moglo bi dodatno unaprediti tačnost podataka.

7. LITERATURA

[1] Li, Edmond, et al. "Electronic health records, interoperability and patient safety in health systems of high-income countries: a systematic review protocol." BMJ open 11.7 (2021): e044941.

[2] Clement, Tosin, et al. "Cyber Analytics: Modelling the Factors Behind Healthcare Data Breaches for Smarter Security Solutions." International Journal of Advance Research, Ideas and Innovations in Technology 10.1 (2024): 49-75.

[3] Bashir, Imran. Mastering blockchain. Packt Publishing Ltd, 2017.

[4] RASEL, MD, and Revathi Bommu. "Blockchain-Enabled Secure Interoperability: Advancing Electronic Health Records (EHR) Data Exchange." International Journal of Advanced Engineering Technologies and Innovations 1.3 (2024): 262-281.

[5] Sarmah, Simanta Shekhar. "Understanding blockchain technology." Computer Science and Engineering 8.2 (2018): 23-29.

[6] Hyperledger Fabric docs., [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5. [Accessed 9 2024].

[7] Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." 2016 2nd international conference on open and big data (OBD). IEEE, 2016.

[8] Quaini, Tiago, et al. "A MODEL FOR BLOCKCHAIN-BASED DISTRIBUTED ELECTRONIC HEALTH RECORDS." IADIS International Journal on WWW/Internet 16.2 (2018).

[9] Capece, Guendalina, and Francesco Lorenzi. "Blockchain and Healthcare: Opportunities and Prospects for the EHR." *Sustainability* 12.22 (2020): 9693.

[10] HAPI FHIR, [Online]. Available: https://hapifhir.io/. [Accessed 9 2024].

Kratka biografija:

Lea Stamenković je rođena 26. 6. 1999. u Subotici. Osnovne akademske studije je završila 2022. godine na Fakultetu tehničkih nauka u Novom Sadu. Master rad na Fakultetu tehničkih nauka iz oblasti Računarstva i automatike – Elektronsko poslovanje odbranila je 2024. godine.
kontakt: lea.stamenkovic99@gmail.com