OSIGURANJE KVALITETA I SIGURNOSTI PODATAKA ZA DIGITALNE CERTIFIKATE U VISOKOM OBRAZOVANJU

ENSURING DATA QUALITY AND SECURITY FOR DIGITAL DIPLOMA CERTIFICATES IN HIGHER EDUCATION

Denis Čeke, Nevzudin Buzađija
Politehnički fakultet, Univerzitet u Zenici
Zenica
Bosna i Hercegovina

Suad Kunosić
Prirodno-matematički fakultet,
Univerzitet u Tuzli
Tuzla
Bosna i Hercegovina

REZIME

Podaci o studentima, njihovim postignućima tokom studija i završnoj kvalifikaciji (diplomi) jedan su od najvažnijih podataka na univerzitetima. Osiguranje kvaliteta podataka visokog obrazovanja moguće je uz pomoć savremenih tehnologija pohrane podataka, pri čemu se, uz klasične baze podataka, na naučnoj sceni pojavljuju i nove tehnologije. Trenutno, jedna od najznačajnijih tehnologija u ovom kontekstu je blockchain tehnologija. U ovom radu predstavit će se mogućnosti korištenja Hyperledger Fabric blockchain platforme za očuvanje konzistentnosti i sigurnosti podataka studenata i njihovih završnih kvalifikacija nakon završetka studija.

Ključne riječi: diplome, sigurnost, blockchain, hyperledger fabric

ABSTRACT

Data on students, their achievements during their studies, and the final qualification (diploma) represent one of the most important data elements in higher education institutions. Ensuring the quality of HEI data is possible with the help of modern data storage technologies, where, in addition to classic databases, new technologies appear on the scientific scene. Currently, one of the most significant technologies in this context is blockchain technology. This paper will present the possibilities of using the Hyperledger Fabric blockchain platform to preserve the consistency and security of students' data and their final qualifications upon completion of studies.

Keywords: diploma certificates, security, blockchain, hyperledger fabric

1. UVOD

Zaštita i očuvanje privatnosti ličnih podataka predstavlja jedan od glavnih zahtjeva kada se radi o bilo kojoj aplikaciji koja se bavi obradom takvih podataka. Informacioni sistemi koji čuvaju i obrađuju podatke o studentima u sistemima visokog obrazovanja imaju iste zahtjeve. Javno izlaganje ovakvih podatka predstavlja oblik jedne ozbiljne prijetnje po sigurnost studenata kao i njihovog statusa unutar sistema visokog obrazovanja. Iz ovog razloga je potrebno iskoristiti mogućnost naprednih tehnologija kako bi se sigurnost podataka podigla na najviši nivo. U posljednjih nekoliko godina došlo je do značajnog porasta upotrebe i primjene rješenja na osnovi korištenja blockchain tehnologija u svim sferama društva, od transporta, zdravstva, logistike pa i do upotrebe u sistemima za obradu digitalnih certifikata odnosno u

sferi obrazovanja sa akcentom na visoko obrazovanja. Ovaj trend je dostigao svoj vrhunac kada je došlo do pojave povećanog broja krivotvorenih dokumenata sa jedne strane, a sa druge strane imamo jako veliki izražaj kibernetičkih napada na infrastrukture od javnog i industrijskog značaja. Kada je u pitanju protok informacija unutar samih institucija, posebno se stavlja akcenat za razmjenom tačnih i nepromijenjenih podataka. Za rješenja ovakvog problema potreban je sistem ili platforma koji će na sistematičan, siguran i pouzdan način učiniti da imamo osiguran ovakav način komunikacije i smještanja podataka. Blockchain tehnologija predstavlja jedno od mogućih rješenja koje ispunjava sve prethodno navedene potrebe. Jedna od takvih privatnih blockchain mreža jeste i Hyperledger Fabric [1] koja se do sada pokazala kao jedna od najpouzdanijih platformi kada su u pitanju oblasti primjene kao što su zdravstvo, školstvo, logistika [2,3,4,5,6] itd. Važno je naglasiti da je u ovom slučaju kvaliteta i konzistentnost podataka osigurana upotrebom blockchain tehnologije. U ovom radu prikazana je mogućnost korištenja jedne ovakve platforme za potrebe sigurnog i trajnog smještanja podataka unutar sistema jedne visokoškolske institucije na temelju blockchain tehnologije.

2. TEHNOLOGIJE ZA PODRŠKU PREDLOŽENOM MODELU SISTEMA

Tehnologija koja služi kao podrška razvoju jednog ovakvog sistema je platforma Hyperledger Fabric koja je bazirana na blockchain tehnologiji.

2.1. Blockchain

Blockchain se može definirati kao nepromjenjiva knjiga za bilježenje transakcija, koja se održava unutar distribuirane mreže međusobno nepovjerljivih čvorova. Svaki čvor u mreži održava svoju kopiju glavne knjige. Blockchain je povezana lista podatkovnih blokova, koji uvijek sadrže pokazivač na prethodni blok. Prilikom razmjene transakcija ne postoji nikakav regulator osim same mreže koja sadrži informacije o svim transakcijama koje su ikada izvedene [7].

Blockchain platforme se općenito mogu podijelili u dvije osnovne grupe: javne ili otvorene (*Public/Permissionless*) i privatne ili zatvorene (*Private/Permissioned*) blockchain.

U javnom blockchain sistemu bilo koji anonimni korisnik može se pridružiti mreži a konsenzus se postiže putem različitih algoritama koji su bazirani na tome da članovi mreže ulažu svoje računarske resurse u rješavanje kriptografske, matematičke zagonetke i na taj način se sprječava da itko od članova ima dominaciju nad sistemom.

Privatne blockchain mreže su sistemi zatvorenog tipa u kojima se konsenzus ne određuje pomoću algoritma nego svaki član daje podatke o sebi da postane dio mreže, da koristi mrežu i šalje transakcije preko mreže. Ova vrsta blockchian sistema je napravljena sa razlogom da se omogući organizaciji ili konzorcijumu organizacija da što efikasnije izmjenjuju informacije i trajno bilježe sve operacije na mreži.

2.2. Hyperledger fabric

Hyperledger Fabric (HF) [8] je platforma otvorenog koda, namijenjena korporativnoj upotrebi i temeljena na tehnologiji distribuirane knjige zapisa (engl. *distributed ledger*), a pruža određene ključne mogućnosti koje ne nude popularne blockchain tehnologije. HF ima modularnu i podesivu arhitekturu, te preko svojih alata omogućava inovacije, optimizaciju i prilagodljivost za razne industrijske sektore. HF podržava pametne ugovore (engl. *smart contracts*) koji su pisani u jezicima opće namjene kao što su *Java*, *Go* i *JavaScript*. HF je također platforma zatvorenog tipa (engl. *permissioned*) što znači da se za razliku od javne mreže, sudionici se poznaju i nisu anonimni, te trebaju imati dozvolu za sudjelovanje u mreži.

Osnovni koncepti Hyperledger Fabric mreže su [9]: *Assets* – imovina su entiteti koji se razmjenjuju na mreži; *Chaincode* – lančani kôd je softver koji definira instrukcije i pravila za modificiranje globalnog stanja na mreži; *Ledger* – distribuirana glavna knjiga je knjiga transakcija koja sadrži zapise o svim transakcijama koje su se dogodile na mreži; *Consensus* – konsenzus predstavlja specifični algoritam na osnovu kojega svi članovi mreže zajedno postižu sporazum i donose odluku o akcijama na mreži; *Channels* - kanal je dio mreže koji omogućava da dvoje ili više članova mreže može uspostaviti privatnu komunikaciju i preko kanala slati podatke kojima samo članovi tog kanala mogu pristupati.

3. PREDLOŽENI MODEL SISTEMA

Predloženi model sistema se sastoji iz dva osnovna segmenata: informacionog sistema univerziteta (ISU) i Hyperledger Fabric testne aplikacije. Informacioni sistem, kao takav, već postoji unutar univerziteta i služi za generisanje podataka o diplomiranim studentima koji se zatim u učitavaju u Hyperledger Fabric blockchain mrežu. Podaci koji se preuzimaju/izvoze iz ISU (u *excel* formatu dokumenta – nazivi kolona tabele) su sljedeći: broj diplome (*diplomaNumber*), ime i prezime studenta (*studentFirstLastName*), jedinstveni ID studenta (*studentID*), broj indeksa (*indexNumber*), datum rođenja (*birthDate*), mjesto rođenja (*birthPlace*), ciklus studija (*graduationLevel*), ocjena sa kojom je student diplomirao (*graduationGrade*), i datum diplomiranja (*graduationDate*). Na slici 1 dat je šematski prikaz potencijalne realizacije cjelokupnog sistema.

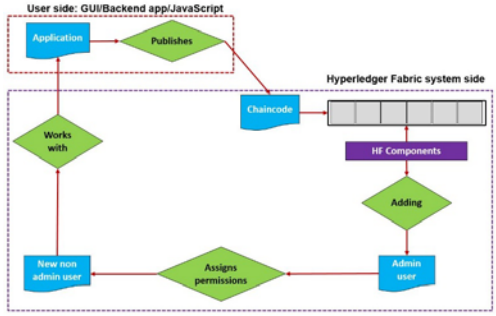
Slika 1. Shematski prikaz prijedloga implementacije sistema

3.1. Hyperledger Fabric platforma za potporu smještanja digitalnih diploma

Razvoj programske potpore za digitalizaciju podataka o diplomama studenata na Hyperledger Fabric platformu, sastoji se od nekoliko faza. Prva faza obuhvata razvoj *chaincode* aplikacije, što je u suštini ekvivalent razvoju pametnih ugovora kod Ethereum platforme. Dakle, svaki ugovor ili forma sa podacima koja se treba postaviti na blockchain se postavlja putem *chaincode* dijela HF platforme. Razvoj HF aplikacije kod koje korisnik treba da unosi podatke putem terminala i u određenom formatu koji je propisan od strane HF fondacije, predstavlja težak posao. Iz ovog razloga, HF fondacija je uspostavila podršku za razvoj i korištenje *chaincode* dijela sistema ali u nekom od opće prihvaćenih programskih jezika, kao što su *Go*, *JavaScript* i *Java*. Predefinirani jezik za rad sa HF platformom je *Go* programski jezik, ali se kroz definiciju rada sa sistemom mogu koristiti i *JavaScript* ili *Java*. Druga faza razvoja sistema predstavlja programiranje dijela aplikacije koja će da komunicira sa *chaincode* dijelom sistema. Za potrebe ovog rada, korišten je *JavaScript* programski jezik uz čiju pomoć je razvijena kompletna poslovna logika aplikacije. U svrhu kreiranja što jednostavnije radnog okruženja za krajnjeg korisnika, u trećoj fazi razvijen je GUI dio aplikacije koji kao svoju osnovu koristi *pug* [10] sistem za generisanje HTML predložaka. U svrhu testiranja i demonstracije rada aplikacije, za razvoj testnog web servera korišteno je *Express.js* [11] razvojno okruženje.

Svaka aktivnost koja se treba izvršiti na mreži, mora biti odobrena od strane samog korisnika mreže. Taj korisnik mora biti dodijeljen od strane administratora mreže na samoj mreži. Za korisnika i za administratora se moraju kreirati certifikati za pristup mreži. Ti certifikati se

generišu pomoću kôda koji je postavljen od strane HF fondacije [12,13] a što je urađeno i ovom predloženom modelu sistema. Na slici 2 prikazana je strukturalna organizacija načina interakcije korisnika sa HF sistemom.



Slika 2. Shematski prikaz interakcije korisnika sa Hyperledger Fabric

Dio izvornog kôda aplikacije napisanog za *chaincode*, dat je na slici 3 i prikazuje način kako se piše izvorni kôd aplikacije za dohvatanje neke određene diplome sa HF blockchain mreže. Na slici 4 prikazana je funkcija pomoću koje smještamo novu diplomu na HF blockchain mrežu.

```
async queryDiploma(ctx, diplomaNumber) {
// get the diploma from chaincode state
const diplomaAsBytes = await ctx.stub.getState(diplomaNumber);
if (!diplomaAsBytes || diplomaAsBytes.length === 0) {
            throw new Error(`${diplomaNumber} does not exist`);}
        console.log(diplomaAsBytes.toString());
        return diplomaAsBytes.toString(); }
```

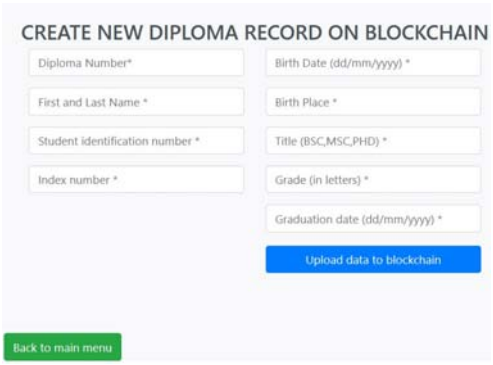
Slika 3. Dohvatanje zapisa o diplomi iz HF blockchain mreže (izvadak kôda)

```
async createDiploma(ctx, diplomaNumber, studentFirstLastName, studentID, indexNumber,
birthDate, birthPlace, graduationLevel, graduationGrade, graduationDate) {
console.info('============= START : Create Diploma Certificate ===========');
        const diploma = {
            studentFirstLastName, docType: 'diploma', studentID, indexNumber, birthDate,
            birthPlace, graduationLevel, graduationGrade, graduationDate
        };
await ctx.stub.putState(diplomaNumber, Buffer.from(JSON.stringify(diploma)));
console.info('============= END : Create Diploma Certificate ===========');
}#
```

Slika 4. Izrada novog zapisa diplome na HF blockchain mreži (izvadak kôda)

Funkcije koje su napravljene unutar HF platforme omogućavaju kreiranje i upotrebu *chaincode* elemenata sistema. Za uspješno kreiranje funkcionalnosti sistema potrebno je pratiti upute HF fondacije vezano za korištenje ovih API funkcionalnosti [14]. Poslovna logika u ovom slučaju ima svoj predefinirani predložak koji je potrebno pratiti kako bi se kreirao funkcionalni dio aplikacije zadužen za komunikaciju sa HF blockchain.
Nakon što je aplikacije napravljena i pokrenuta na web serveru, kreirani *chaincode* (slike 3 i 4) se publikuje na HF blockchain i sa njime se vrši interakcija putem spomenute aplikacije.

Forma za unos novog certifikata za studenta koja je u pozadini povezana sa klijentskim *JavaScript* kodom aplikacije, prikazana je na slici 5. Forma u suštini služi samo kao pojednostavljeni grafički interfejs za komunikaciju sa ostatkom sistema. Naravno, ovi podaci su prethodno izvezeni iz informacionog sistema univerziteta u *excel* formatu dokumenta u odgovarajućoj formi, a nakon detaljnog pregleda i utvrđivanja njihove ispravnosti, oni su pripremljeni za slanje na privatni HF blockchain sistem a što se u trenutnoj verziji sistema obavlja ručno bez značajnijeg stepena automatizacije procesa.



Slika 5. Forma za dodavanje novog zapisa u HF blockchain

3.2. Prednosti i nedostatci predloženog model sistema

HF, koji čini glavnu komponentu predloženog modela sistema, je sistem koji ima nekoliko značajnih osobina koje su izuzetno važne u oblastima primjene kao što su institucije visokog obrazovanja, a to je da: ima podršku za upotrebu u sistemima velikih kompanija, ima modularnu arhitekturu koja omogućava razvoj dodatnih elemenata, za komunikaciju između stranaka koriste se privatni komunikacijski kanali, i ima mogućnost korištenja pametnih ugovora koji se kod HF zovu lančani kod (engl. *chaincode*). Također, ne postojanje kripto valute unutar samog sistema niti potrebe za njenim korištenjem u toku rada sa sistemom, ovu platformu čini izuzetno prihvatljivom za upotrebu u sistemima velikih kompanija za potrebe razvoja i upotrebe njihovih poslovnih aplikacija.

Hyperledger Fabric je prilično nova tehnologija pa stoga je potreban i značajan nivo znanja za razvoj i implementaciju sistema koji su na njemu bazirani. Jedan od nedostataka predloženog modela sistema leži u činjenici da razvoj i implementacija jednog ovakvog rješenja zahtjeva poznavanje više različitih tehnologija, od blockchain tehnologije sa akcentom na HF, pa sve do razvoja poslovne logike u nekom od programskih jezika i na kraju same implementacije u nekom produkcijskom okruženju.

Međutim, HF je jedna od vodećih platformi koja na sve moguće načine nastoji ovako visoku složenost jednog ovakvog sistema što više približiti klasičnom programeru kako bi razvoj i implementacija jednog ovakvog sistema bila što jednostavnija čime se ujedno pokušava prevazići jedna od osnovnih prepreka trenutno široj popularizaciji HF platforme.

4. DALJNJA ISTRAŽIVANJA

Trenutno razvijeni sistem je još uvijek u testnoj fazi pa je samim time i njegova komunikacija sa informacionim sistemom univerziteta (ISU) još uvijek jako malo automatizirana. U daljnjem radu i istraživanju težiti će se potpunijem i značajnijem automatiziranom procesu integracije HF sa ISU, prvenstveno zbog brzine izvršavanja svih procesa, a s druge strane i zbog smanjenja mogućih grešaka u prijenosu podataka iz ISU u HF. Prvi koraci testiranja

sistema pokazali su nam da se jedan ovakav sistem zasigurno može realizirati i integrirati u postojeće informacione sisteme bilo kojeg univerziteta.

5. ZAKLJUČAK

Očuvanje kvaliteta i integriteta podataka predstavlja jednu od najvažnijih karakteristika koju treba da ima neki informacioni sistem koji se koristi za čuvanje podataka čiji sadržaj i kontekst ne smije biti izmijenjen na bilo koji način. U ovom radu prezentirana je mogućnost upotrebe blockchain tehnologije, tačnije privatnog blockchain sistema, Hyperledger Fabric, u svrhu očuvanja prvenstveno integriteta a samim time i kvaliteta podataka vezanih za diplome studenata u sistemu visokog obrazovanja. Obzirom na današnju učestalost kibernetičkih napada na informacione sisteme, kompromitovanje korisničkih i drugih podataka, blockchain sistem, zbog svoje arhitekture i načina realizacije, predstavlja jedan od sistema koji se može pohvaliti prilično velikim stepenom otpornosti na ovakve prijetnje. Softverska rješenja bazirana na blockchain tehnologiji omogućavaju povećanje sigurnosti i pouzdanosti podataka u svim sferama privrede, zdravstvenom sektoru, logističkim lancima opskrbe pa i u sistemima obrazovanja.

6. REFERENCE

[1] "Hyperledger Fabric – Hyperledger Foundation." https://www.hyperledger.org/use/fabric (accessed Jan. 17, 2023).

[2] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002.

[3] D. Khan, L. T. Jung, M. A. Hashmani, and M. K. Cheong, "Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises," *Sensors*, vol. 22, no. 3, Feb. 2022, doi: 10.3390/s22030915.

[4] C. Reis-Marques, R. Figueiredo, and M. de Castro Neto, "Applications of Blockchain Technology to Higher Education Arena: A Bibliometric Analysis," *Eur. J. Investig. Health Psychol. Educ.*, vol. 11, no. 4, pp. 1406–1421, Nov. 2021, doi: 10.3390/ejihpe11040101.

[5] "Blockchain Technology – Prospects, Challenges and Opportunities - IEEE Blockchain Initiative." https://blockchain.ieee.org/technicalbriefs/june-2019/blockchain-technology-prospects-challenges-and-opportunities (accessed Jan. 17, 2023).

[6] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[7] "Ledger — hyperledger-fabricdocs main documentation." https://hyperledger-fabric.readthedocs.io/en/release-2.4/ledger/ledger.html (accessed Feb. 13, 2023).

[8] "Introduction — hyperledger-fabricdocs main documentation." https://hyperledger-fabric.readthedocs.io/en/release-2.5/blockchain.html?highlight=blockchain#what-is-a-blockchain (accessed Feb. 13, 2023).

[9] "Hyperledger Fabric Model — hyperledger-fabricdocs main documentation." https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric_model.html (accessed Jan. 18, 2023).

[10] "Getting Started – Pug." https://pugjs.org/api/getting-started.html (accessed Feb. 13, 2023).

[11] "Express - Node.js web application framework." https://expressjs.com/ (accessed Feb. 13, 2023).

[12] "Hyperledger Fabric – Hyperledger Foundation." https://www.hyperledger.org/use/fabric (accessed Feb. 13, 2023).

[13] "Hyperledger Fabric Samples." Hyperledger, Feb. 13, 2023. Accessed: Feb. 13, 2023. [Online]. Available: https://github.com/hyperledger/fabric-samples

[14] "Fabric Contract APIs and Application APIs — hyperledger-fabricdocs main documentation." https://hyperledger-fabric.readthedocs.io/en/latest/sdk_chaincode.html (accessed Feb. 13, 2023).