Razvoj programske podrške za digitalne studentske bedževe na javnom blockchainu

Grabar, Antonia

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Preddiplomski studij računarstva

Završni rad

Razvoj programske podrške za digitalne studentske bedževe na javnom blockchainu

Rijeka, rujan 2022.

Antonia Grabar
0069088321

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Preddiplomski studij računarstva

Završni rad

Razvoj programske podrške za digitalne studentske bedževe na javnom blockchainu

Mentor: prof.dr.sc. Kristijan Lenac

Rijeka, rujan 2022.

Antonia Grabar
0069088321

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
POVJERENSTVO ZA ZAVRŠNE ISPITE

Rijeka, 15. ožujka 2022.

Zavod: **Zavod za računarstvo**
Predmet: **Operacijski sustavi**
Polje: **2.09 Računarstvo**

ZADATAK ZA ZAVRŠNI RAD

Pristupnik: **Antonia Grabar (0069088321)**
Studij: Preddiplomski sveučilišni studij računarstva

Zadatak: **Razvoj programske podrške za digitalne studentske bedževe na javnom blockchainu / Development of digital student badges on public blockchain**

Opis zadatka:

Osmisliti i izraditi mobilnu i web aplikaciju u obliku blockchain novčanika za primanje, pregledavanje i upravljanje digitalnim studentskim bedževima na javnoj blockchain mreži.

Rad mora biti napisan prema Uputama za pisanje diplomskih / završnih radova koje su objavljene na mrežnim stranicama studija.

Zadatak uručen pristupniku: 21. ožujka 2022.

Mentor:

Prof. dr. sc. Kristijan Lenac

Predsjednik povjerenstva za završni ispit:

Prof. dr. sc. Kristijan Lenac

Izjava o samostalnoj izradi rada

Izjavljujem da sam samostalno izradio ovaj rad.

Rijeka, rujan 2022.

Ime Prezime

Zahvala

Zahvaljujem mentoru prof.dr.sc. Kristijanu Lencu na podršci tijekom pisanja ovoga rada, kao i korisnim savjetima. Zahvaljujem obitelji i kolegama na neizmjernoj podršci tijekom studiranja.

Sadržaj

Popis slika

Poglavlje 1

Uvod

Nastanak blockchain tehnologije postavio je temelj revolucionarnom načinu dokazivanja vlasništva i pohranjivanja podataka koji se ne mogu promijeniti ni hakirati. Sva moć odlučivanja pripala je distibuiranoj mreži ljudi umjesto centralnom entitetu, što osigurava transparentnost, legitimnost i nepromjenjivost povijesti bilo koje digitalne imovine. Mnogi ljudi se ne osjećaju spremno koristiti kriptovalute i tokene samo zato što ne razumiju tehnologiju koja ih podržava. Iz tog razloga bitno je upoznati ljude sa svim prednostima blockchaina kako bi se povećala vjerojatnost da ljudi prihvate ideju decentraliziranih sistema i novog načina dokazivanja vlasništva.

Projekt digitalnih studentskih bedževa iniciran je od strane Tehničkog fakulteta Sveučilišta u Rijeci kako bi studentima približio blockchain tehnologije te istovremeno povećao njihovu motiviranost za aktivan doprinos studentskim zajednicama. Pojam studentskih bedževa odnosi se na nezamjenjive tokene - vizualne digitalne uradke trajno zapisane na javni blockchain koji su jedinstveni i vezani uz identitet osobe. Postojat će desetak različitih vrsti bedževa, pa će tako studenti biti nagrađeni za postignuća ostvarena tijekom studiranja, sudjelovanje na konferencijama te članstva u studentskim timovima i organizacijama. Na primjer, student koji prezentira rad na konferenciji dobiva u trajno vlasništvo bedž "Academic author 2022", a ukoliko je primljen u studentski tim dobiva bedž s oznakom "RBT member 2022". Nakon isteka članstva, bedževi neće postati neaktivni, već će ih studenti moći držati neograničeno dugo.

1.1 Opis zadatka

Zadatak završnog rada bio je izraditi aplikaciju koja će studentima omogućiti spajanje sa njihovim kripto novčanikom na Ethereum ili Cardano mreži te pregled svih njihovih bedževa sa pripadajućim metapodacima. Studentski bedževi već su bili izrađeni, stoga je cilj ovog rada bio pronaći najbolji način za njihovo prikazivanje, kao i tehnologije koje će to omogućiti. Također, u ovom radu će se promotriti osnovni koncepti blockchain tehnologije, usporediti značajke Ethereum i Cardano mreže te opisati utjecaj nezamjenjivih tokena na svakodnevni život.

Poglavlje 2

Blockchain

Ideja blockchain-a kao novog decentraliziranog načina provođenja transakcija prvi puta je predstavljena u revolucionarnom radu *Bitcoin: A Peer-to-Peer Electronic Cash System* autora pod pseudonimom Satoshi Nakamoto. U radu je objašnjen prijedlog uvođenja elektroničke gotovine koja bi omogućila izravna plaćanja od jedne strane do druge bez prolaska kroz financijsku instituciju. Uz digitalni novac, predstavljen je revolucionaran oblik peer-to-peer mreže koja uvodi mehanizam računalnog dokaza kronološkog slijeda transakcija kako bi se sustav zaštitio od mogućih napadača. [1]

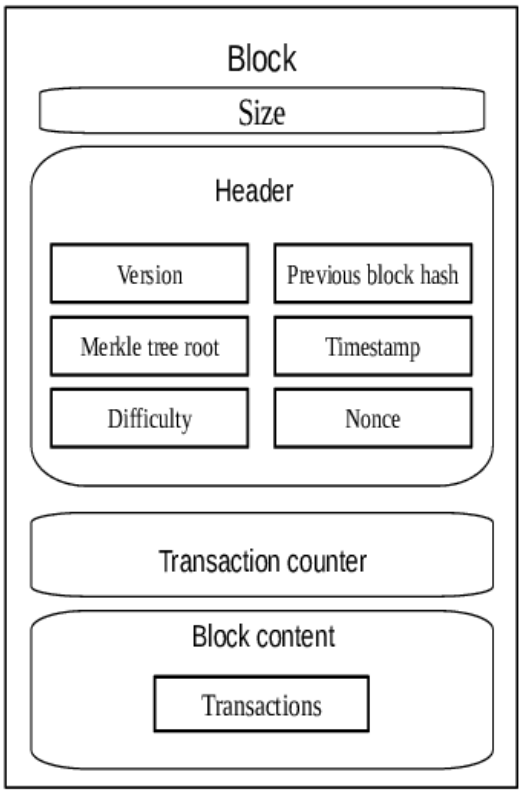
2.1 Struktura

Ključna razlika tipične baze podataka i blockchaina je način strukturiranja podataka. Dok su u bazi podataka podaci organizirani u tablice, blockchain organizira podatke u blokove. Nakon što blokovi ispune svoj kapacitet podacima, zatvaraju se te povezuju s prethodno popunjenim blokom tvoreći lanac blokova. Lanci blokova su također poznati kao tehnologija distibuirane knjige (engl. *Distributed Ledger Technology - DLT*) zbog evidencije transakcija koje se ne mogu mijenjati, brisati ili uništiti. [2]

Svaki individualni blok sastoji se od 4 komponente: veličine bloka, zaglavlja, broja trenutno pohranjenih transakcija te liste transakcija. Shematski prikaz strukture bloka vidljiv je na slici 2.1.

Zaglavlje bloka ujedno je najbitnija komponenta jer se koristi za identifikaciju pojedinog bloka u lancu. Sastoji se od slijedećih dijelova: [3]

- **Verzija** - Broj verzije opisuje pravila validacije koja taj blok slijedi. Ako se broj verzije bloka razlikuje od ostalih blokova, oni ne mogu biti dio istog blockchaina.
- **Hash prethodnog bloka** - 32-bajtno polje koje sadrži hash, tj. kriptirani broj zaglavlja prethodnog bloka. Povezivanje hash-ova ono je što osigurava sigurnost bloka i otpornost na neovlašteno korištenje.
- **Merkleov korijen** - Hash izveden iz hash-ova svih transakcija uključenih u pojedini blok. Ova primjena kriptografije osigurava da se nijedna od transakcija ne može izmijeniti bez izmjene cijelog zaglavlja.
- **Vremenska oznaka** - Glavna funkcija vremenske oznake jest određivanje točnog trenutka odvijanja nekog događaja poput rudarenja bloka ili validacije od strane mreže.
- **Težina** - 4-bajtna datoteka koja određuje težinu matematičke zagonetke čije je rješenje potrebno za uključivanje bloka u blockchain. Težina se povećava proporcionalno broju ljudi uključenih u proces kako bi se regulirala ponuda kriptovalute.
- ***Nonce*** - Polje *nonce* je 4-bajtni broj koji se inkrementira s namjerom rješavanja matematičke zagonetke uključivanja bloka u blockchain.



Slika 2.1 Struktura bloka.

2.2 Mehanizmi konsenzusa

Javne blockchain mreže su u potpunosti globalni decentralizirani sustavi koji rade bez pojedinačnih autoriteta te uključuju doprinose stotina tisuća sudionika. U takvom dinamičnom sustavu nužan je učinkovit, pouzdan i siguran mehanizam kako bi se osigurala autentičnost svih transakcija na mreži te legitimnost doprinosa čvorova blockchaina. Ovu važnu zadaću obavlja skup posebno definiranih pravila nazvan mehanizam konsenzusa. U kontekstu blockchaina i kriptovaluta, dokaz o radu (engl. *Proof of Work*) i dokaz o udjelu (engl. *Proof of Stake*) dva su najčešća mehanizma konsenzusa.[4]

2.2.1 Proof of Work

Kako novi oblici tehnologije i novca postaju javno dostupni, loši aktori nastoje iskoristiti njihove propuste za osobnu financijsku korist. Nastankom digitalne valute pojavio se problem poznat pod nazivom dvostruka potrošnja (engl. *double-spending*). Dvostruka potrošnja je mogućnost da netko umnoži digitalni novac i potroši ga istovremeno na dva ili više mjesta. [5] Kako bi riješio taj problem, Nakamoto uvodi mehanizam konsenzusa poznatiji kao dokaz o radu (engl. *Proof of Work*).

Dokaz o radu zahtijeva od sudionika mreže da ulože napor u rješavanje proizvoljne matematičke zagonetke kako bi postigli konsenzus na decentraliziran način i spriječili bilo koga da zavara sustav. Rješavanje zagonetke uključuje nasumično generiranje što više *nonce* brojeva te zahtijeva ogromnu količinu električne energije. Prvi sudionik čiji nonce generira hash koji je manji ili jednak ciljnom hash-u dobiva nagradu u kriptovaluti tog blockchaina te dodaje novi blok u blockchain. Opisan proces poznat je kao "rudarenje", dok su sudionici procesa nazvani "rudari".[1]

Budući da svaki od blokova sadrži svoju vremensku oznaku, implementacijom dokaza o radu mreža postaje kronološki slijed transakcija potvrđen najvećim skupom CPU snage. Promjena bilo kojeg aspekta blockchaina znatno je otežana budući da bi svaki pokušaj krivotvorenja uzrokovao promjenu svih prethodnih blokova. Sustav će biti siguran sve dok pošteni čvorovi kontroliraju više CPU snage nego bilo koja grupa čvorova napadača.

2.2.2 Proof of Stake

Za razliku od dokaza o radu koji od sudionika zahtijeva da obavi određenu količinu računalnog rada, u dokazu o udjelu (engl. *Proof of Stake*) sudionik mora položiti određenu svotu kriptovalute u ugovor o depozitu kako bi postao validator. Stvaranje novih blokova podijeljeno je na vremenske intervale te se u svakom vremenskom intervalu nasumično bira validator koji je odgovoran za stvaranje novog bloka i njegovo slanje drugim čvorovima na mreži. Također, bira se skup validatora čiji se glasovi koriste za validiranje predloženog bloka, a težina glasa validatora ovisi o veličini njegovog depozita.[6]

Prijetnja od napada i dalje postoji na dokazu o udjelu kao i na dokazu rada, ali je neučinkovita i riskanta za napadače. Napadač bi trebao imati 51% uložene kriptovalute (kod Ethereum mreže ovaj iznos doseže 15 bilijuna američkih dolara). Uz to, pošteni validatori mogu nastaviti graditi na manjinskom lancu i ignorirati novonastale promjene napadača. Također mogu odlučiti nasilno ukloniti napadače s mreže i uništiti njihovu uloženu kriptovalutu.[6]

2.3 Ethereum

Povijest Ethereuma seže do 2013. godine kada je kanadski programer Vitalik Buterin predložio platformu s ugrađenim Turing-kompletnim programskim jezikom, koji bi svakome omogućio pisanje pametnih ugovora i decentraliziranih aplikacija. Od njegovog pokretanja 2015. godine, Ethereum nikad nije pretrpio zastoje te danas broji preko 2970 projekata, 50.5 milijuna pametnih ugovora i 71 milijun kripto novčanika sa određenim iznosom *ethera*, kriptovalute Ethereuma. Ethereum trenutno pokreće Proof of Work mehanizam konsenzusa. [7]

Za razliku od Bitcoina koji je distribuirana knjiga, Ethereum je distribuirani konačni automat. Naime, u Ethereumu postoji globalno virtualno računalo zaslužno za pohranjivanje ogromne podatkovne strukture svih računa i stanja, nazvano *Ethereum Virtual Machine - EVM*. U bilo kojem bloku u lancu, Ethereum ima jedno i samo jedno 'kanonsko' stanje, a EVM je ono što definira pravila za izračunavanje novog valjanog stanja od bloka do bloka. Svaki Ethereum čvor čuva kopiju stanja EVM-a te može zatražiti izvršavanje proizvoljnog koda, koji će nakon izvršavanja promijeniti stanje EVM-a. Također, jedna od najbitnijih zadaća EVM-a je izvršenje i implementacija pametnih ugovora.[8] Korisnicima je tako u nekoliko linija programskog koda omogućeno proizvoljno kodiranje funkcija stanja, kao i iskorištavanje naprednih mogućnosti Ethereuma u decentraliziranim aplikacijama.

2.3.1 Pametni ugovori

Pametni ugovor (engl. *smart contract*) jednostavno je program koji radi na Ethereum blockchainu. To je zbirka koda (njegove funkcije) i podataka (njegovo stanje)

koja se nalazi na određenoj adresi na Ethereum blockchainu.[9] Drugim riječima, pametni ugovor je skripta koja se poziva određenim parametrima te izvodi računanja ukoliko su ispunjeni određeni uvjeti. Svaki programer može napisati pametni ugovor u jednom od Etehreumovih programskih jezika (najpoznatiji je Solidity) i postaviti ga na mrežu uz uvjet da pokrije troškove transakcije za njegovu implementaciju. Nakon kompajliranja, programeri učitavaju pametne ugovore u EVM stanje, gdje drugi korisnici mogu zatražiti njihovo izvršavanje s različitim parametrima.

Budući da su pametni ugovori dijelovi računalnog koda bez mogućnosti slanja HTTP zahtjeva, ne mogu izravno dobiti informacije o vanjskom svijetu. Ta prepreka zaobilazi se posebnim pružateljima podataka, *oracles*. Bitno je napomenuti da to nisu sami izvori podataka, već slojevi koji pronalaze i autentificiraju vanjske izvore podataka koje zatim daju na pristup blockchainu. *Oracles* se dijele na softverske i hardverske. Softverski isporučuju podatke sa web stranica, poslužitelja ili baza podataka (npr. tečajevi, fluktuacije cijena), dok hardverski prenose informacije iz stvarnog svijeta preko sučelja (npr. senzori, skeneri).[10]

Jedna od najvećih prednosti pametnih ugovora jest eliminiranje potrebe za trećom stranom, to jest posrednikom čija je zadaća potvrđivanje valjanosti dogovora. Kada se obje strane uključene u pametni ugovor slože s njegovim uvjetima, program će se automatski izvršiti. Automatizacija izvršavanja minimizira utrošeno vrijeme na ručnu obradu podataka, kao i pogreške koje mogu nastati prilikom obrade. Također, pametni ugovori osiguravaju sigurnost podataka. Svi podaci su šifrirani i duplicirani više puta sprječavajući hakerske napade i gubitak podataka.

S druge strane, najveći nedostatak pametnih ugovora jest da se ne mogu izbrisati, a interakcije sa njima su nepovratne. U potpunosti su ovisni o programerima zaslužnima za njihovo pisanje te ukoliko su postojale greške u kodu, problem s ugovorom se neće moći riješiti. Također, pametni ugovori ne mogu jamčiti stopostotnu pouzdanost zbog mogućih zastoja i prekida blockchain mreže. Iako Ethereum nije nikad pretrpio zastoje, postoji vjerojatnost zastoja novijih blockchain mreža radi nepotpunog razvoja tehnologije. Iako svatko može izraditi pametni ugovor, pametni ugovori na kojima će se temeljiti ključni dijelovi industrija ili tvrtki zahtijevaju visoku razinu tehničke stručnosti te mogu biti skupi za razvoj.

2.3.2 Decentralizirane aplikacije

Decentralizirana aplikacija (dApp) je aplikacija izgrađena na decentraliziranoj mreži koja kombinira pametni ugovor i frontend korisničko sučelje.[11] Drugim riječima, to su aplikacije pisane u bilo kojem programskom jeziku, kod kojih serverski dio aplikacije obavljaju pametni ugovori. Uz decentraliziranost, ono što razlikuje ove aplikacije od standardnih jest njihova izoliranost. Naime, decentralizirane aplikacjie se izvode na EVM-u te bilo koja pogreška u kodu neće utjecati na funkcioniranje blockchain mreže. Također, ove aplikacije su Turing potpune, što znači da uz dobivene resurse mogu izvesti bilo koju radnju te riješiti bilo koji računski problem.

Budući da je pametni ugovor pohranjen na blockchainu, korisnici će uvijek moći pristupiti aplikaciji bez straha od mogućeg zastoja, a zlonamjerni akteri neće moći izvesti napade uskraćivanjem resursa (engl. *Denial-of-service attack - DoS*). Još jedna prednost decentraliziranih aplikacija je potpuna sloboda i privatnost korisnika. Korisnici mogu interagirati s aplikacijom bez pružanja osobnih informacija te im je pružena potpuna sloboda podnošenja transakcija i čitanja podataka sa blockchaina.

Upotreba decentraliziranih aplikacija još uvijek je u ranoj fazi, stoga je podložna raznim problemima i nepoznanicama. Najveći problem razvoja takvih aplikacija su poteškoće u mijenjanju programskog koda. Aplikacije će gotovo sigurno zahtijevati razne promjene i poboljšanja, što razvojnim programerima može predstavljati izazov zbog teškog mijenjanja podataka i koda na blockchainu. Također, ukoliko aplikacija zahtijeva veliku količinu računalnih resursa, to može uzrokovati zagušenje mreže radi ograničenja obrade 10-15 transakcija u sekundi. Još jednu prepreku predstavlja korisničko sučelje aplikacije, koje treba biti intuitivno i sadržavati visoku razinu performansi kako bi se mogao mjeriti s dobro poznatim programima sa svrhom poticanja novih korisnika na korištenje decentraliziranih aplikacija.

Ethereum trenutno dominira nad izradom decentraliziranih aplikacija zbog svoje jedinstvene i fleksibilne infrastrukture kojom potiče programere na pronalaženje novih inovativnih upotreba aplikacija. Decentralizirane aplikacije bit će više uključene u svakodnevni život i industrije, smanjujući troškove i eliminirajući treće strane iz mnogih osobnih i poslovnih transakcija.

2.3.3 Prelazak na Proof of Stake

Iako prvobitno pokrenut s Proof of Work mehanizmom konsenzusa, dugogodišnji cilj Ethereuma je prelazak na Proof of Stake mehanizam bez ugrožavanja svoje sigurnosti, stabilnosti i decentraliziranosti. Implementacija rješenja započela je krajem 2020. godine uvođenjem Beacon lanca. Beacon lanac je potpuno neovisna mreža koja ima PoS konsenzusni sloj i pokreće se paralelno s trenutnom glavnom mrežom Ethereum, gdje sloj konsenzusa trenutno ostaje PoW. Održavanjem PoS lanca izoliranim od glavne mreže, rješenje spremno za isporuku se usavršava bez riskiranja funkcionalnosti glavnog Ethereum lanca. Spajanje lanaca nazvano je 'The Merge' te je predviđeno za rujan 2022. godine. Nakon dovršetka spajanja PoW će biti uklonjen, dok će sva Ethereumova povijest ostati sačuvana. [12]

2.4 Cardano

Cardano je open source Proof of Stake blockchain projekt koji je započeo 2015. godine kako bi se pozabavio postojećim blockchain izazovima u dizajnu i razvoju kriptovaluta. Budući da teži rješavanju problema skalabilnosti, interoperabilnosti i održivosti s kojima su se suočavale prva i druga generacija blockchaina, Cardano se smatra blockchainom treće generacije. [13] Nastoji izgraditi mrežu koja će biti dovoljno sigurna da zaštiti podatke milijuna ljudi, dovoljno skalabilna da podrži velik broj transakcija i dovoljno robusna da podrži promjene.

Tehnologija ostvarena kroz znanost utemeljenu na dokazima jedna je od temeljnih značajki Cardano platforme te ono što ju razlikuje od ostalih blockchaina. Primjena rezultata akademskih istraživanja i brojnih formalnih metoda rezultirala je platformom sa impresivnom razinom performansi, kao i jamstvom ispravnosti svojih ključnih komponenti. Svoju stabilnost Cardano zahvaljuje i činjenici da je u potpunosti pisan u programskom jeziku Haskell, koji omogućava pisanje koda pomoću čistih funkcija. Ovakav način pisanja omogućuje nezavisno testiranje komponenti, kao i korištenje čitavog niza naprednih značajki za osiguravanje ispravnosti koda. Također, jedna od najvećih prednosti Cardana jest niska energetska potrošnja, zahvaljujući Proof of Stake mehanizmu.

2021. godine stvoren je Plutus, programski jezik namijenjen za pisanje pametnih ugovora na Cardano mreži. Integracija pametnih ugovora postala je prekretnicom razvoja Cardana, omogućivši izgradnju decentraliziranih aplikacija, stvaranje novih tokena i kriptovaluta te tokenizaciju mnogih vrsta fizičke i digitalne imovine.

2.4.1 Ouroboros

Ouroboros je prvi dokazano siguran Proof of Stake protokol i prvi blockchain protokol koji se temelji na recenziranom istraživanju. Protokol primjenjuje kriptografiju, kombinatoriku i matematičku teoriju igara kako bi zajamčio svoju sigurnost, integritet, dugovječnost, izvedbu i skalabilnost. [14] Temelj Ouroborosa čine skupovi udjela (engl. *stake pools*). Skupovi udjela su poslužiteljski čvorovi koji sadrže kombinirane udjele svojih sudionika te su odgovorni za obradu transakcija i proizvodnju novih blokova.

Ouroboros obrađuje transakcijske blokove dijeleći lance na epohe, koje su dalje podijeljene na vremenske odsječke. Za svaki vremenski odsječak bira se predstavnik koji je zadužen za dodavanje novog bloka u lanac. Biranje predstavnika obavlja se posebnom funkcijom slučajnosti koja u obzir uzima udio udjela sudionika, kao i prethodno generirane vrijednosti slučajnosti već pohranjene u blockchain. Odabran sudionik za uspješno dodan blok dobiva određenu svotu ADE, kriptovalute Cardana. Kako bi povećali vjerojatnost dobivanja nagrade, sudionici mogu delegirati svoj ulog u prethodno spomenute skupove udjela, koji u slučaju stvaranja bloka dijele nagradu među sudionicima, proporcionalno njihovim udjelima. Ovim mehanizmom korisnici se potiču na aktivno sudjelovanje u Cardano mreži uz istovremeno minimiziranje potrošnje energije i računalnih resursa.

Poglavlje 3

Nezamjenjivi tokeni

Nezamjenjivi tokeni (engl *non-fungible tokens - NFT*) kriptografska su imovina na blockchainu s jedinstvenim identifikacijskim kodovima i metapodacima koji ih međusobno razlikuju.[15] Drugim riječima, NFT-jevi dokazuju vlasništvo nad objektima iz stvarnog svijeta poput umjetnosti, glazbe, dokumenata, nekretnina itd. Ono što ih razlikuje od kriptovaluta jest da se ne mogu replicirati te ih se ne može razmjenjivati po ekvivalentnosti.

3.1 Povijest razvoja

Pokušaj stvaranja tokena koji su povezani sa stvarima u stvarnom svijetu i podržani blockchain tehnologijom započeo je 2012. godine objavom rada *Overview of Colored Coins* znanstvenika Meni Rosenfeld. Colored Coins su tokeni nastali na Bitcoin blockchainu s namjerom proširivanja njegovih funkcionalnosti poput atomskih operacija, decentraliziranih mjenjačnica, novog dokazivanja vlasništva te stvaranja kriptovaluta.[16] Međutim, ovi tokeni su vrlo složeni za implementaciju i razvoj zbog ograničenja Bitcoin tehnologije. Također, njihovo uvođenje stvara veliki pritisak na blockchain drastično povećavajući njegovu veličinu i smanjujući njegovu sposobnost obrade transakcija. Ovo su samo neki od faktora zbog kojih se koncept Colored Coins nije nikada mogao realizirati, no postavio je temelje današnjoj implementaciji nezamjenjivih tokena.

Umjetnik Kevin McCoy je 2014. godine na Namecoin blockchainu stvorio pikseliziranu sliku oktagona ispunjenog pulsirajućim koncentričnim krugovima. Slika poznata pod nazivom *Quantum*, danas se smatra prvim NFT-om. Ubrzo nakon stvaranja *Quantuma*, McCoy je zajedno sa suradnikom javnosti predstavio ideju sustava koji bi umjetnicima omogućio potpuno vlasništvo nad svojim djelima. Budući da je ovakav način dokazivanja vlasništva još bio nepoznanica u društvu, javno predstavljanje završilo je ismijavanjem publike. Unatoč tome, eksponencijalno razvijanje NFT tehnologije rezultiralo je prodavanjem ovog djela na dražbi aukcijske kuće Sotheby's za 1.4 milijuna dolara 2021. godine.[17]

Razvoj NFT-jeva na Ethereumu započinje 2017. godine eksperimentalnim projektom *CryptoPunks*. *CryptoPunks* je zbirka od 10 000 algoritamski generiranih i jedinstvenih sličica pikseliziranih ljudskih glava inspiriranih londonskom punk kulturom.[18] Uspjeh ove kolekcije rezultirao je privlačenjem pozornosti javnosti i integracijom NFT-jeva u sve veći broj tehnologija. Ubrzo se otvara mogućnost korištenja kriptovaluta, kao i stečenih NFT-jeva unutar raznih virtualnih igara i platformi. Porast potražnje za NFT-jevima dosegla je vrhunac 2021. godine nakon što su velike aukcijske kuće odlučile prodavati NFT umjetnine za višemilijunske iznose. To je također prethodilo odluci nekolicine blockhaina poput Cardana, Solane, Flowa i Tezosa o implementiranju svoje verzije NFT tehnologije.

3.2 Implementacija

3.2.1 Ethereum

NFT-jevi su najzastupljeniji na Ethereum blockchainu iz više razloga. ERC-721 i ERC1155 su standardi koji su omogućili dodjeljivanje vlasništva i upravljanje prenosivošću NFT-jeva putem pametnih ugovora. Na taj način svim je korisnicima mreže omogućeno jednostavno stvaranje tokena sa jedinstvenim ID-om i metapodacima koji se ne mogu replicirati. Nakon što netko postane vlasnikom određenog NFT-ja, dokaz vlasništva nad originalom postaje dio privatnog ključa njegovog kripto novčanika. Javno dokazivanje povijesti vlasništva je jednostavno zbog javno provjerljive povijesti transakcija i metapodataka NFT-ja. Budući da je metapodacima nemo-

guće manipulirati nakon potvrđene transakcije, vlasništvo se ne može ukrasti. Bitna prednost Ethereuma jest da svi njegovi proizvodi, tj. aplikacije dijele iste dijelove koda, zbog čega su NFT-jevi lako prenosivi na različite proizvode.[19]

Jedna od najvećih prepreka masovnom usvajanju trgovanja NFT-jeva su visoki troškovi transakcija (engl. *gas fees*), koji su izravan rezultat nemogućnosti Ethereuma da provede više od 15 transakcija u sekundi. Troškovi se plaćaju u etheru (ETH), a cijena je izražena u gwei koji je sam po sebi denominacija ETH ($1ETH = 10^9 gwei$).[20] Kad je mreža zagušena, transakcije se natječu za dodavanje u blokove te tada korisnici moraju ponuditi veće troškove kako bi nadmašili konkurentske transakcije. Prilikom velike potražnje, npr. mintanja popularnih NFT kolekcija, troškovi transakcija mogu doseći nekoliko stotina dolara. Iz navedenog razloga korisnici poćinju tražiti jeftinije alternative u ostalim blockchainovima koji implementiraju NFT tehnologije.

3.2.2 Cardano

Za razliku od Ethereuma, NFT-jevi se na Cardano blockchainu stvaraju bez upotrebe pametnih ugovora. Tretiraju se kao svi drugi kripto tokeni te je njihovo stvaranje osnovna ugrađena funkcija samog blockchaina. Direktna posljedica opisanog načina stvranja jest omogućena komunikacija između tokena i ADE zbog istih primjenjenih pravila, smanjenje pogrešaka u programskom kodu te lakša integracija NFT-jeva u decentralizirane aplikacije.[21] Također, odsutnost pametnih ugovora umanjuje troškove koji su potrebni za njihovu implementaciju. Stvaranje NFT-jeva dakle zahtijeva samo osnovni trošak obične transakcije, što čini Cardano isplativijom, bržom i predvidljivijom opcijom od Ethereuma. Isplativosti pridonosi i činjenica da je kreatorima NFT kolekcija omogućeno istovremeno prenošenje tokena na više adresa. Na taj način kreatori plaćaju samo jednu nisku transakcijsku naknadu. Također, jedna od prednosti Cardana jest nedjeljivost metapodataka i tokena. Naime, u ostalim protokolima poput Ethereuma pametni ugovori pohranjuju hash vrijednost koja upućuje na IPFS (engl. *InterPlanetary File System*) ili neku drugu web stranicu koja sadrži metapodatke, to jest atribute NFT-ja. Prilikom stvaranja NFT-ja na Cardanu, metapodaci postaju dio transakcije.

3.3 Primjena

NFT-jevi mogu predstavljati bilo koji tip imovine, uključujući digitalna umjetnička djela, nekretnine, ulaznice za događaje, kolekcionarske predmete, avatare u igrama, diplome itd. NFT tehnologija danas se najviše koristi u digitalnoj umjetnosti te revolucionira način na koji umjetnici mogu stvarati nove projekte i preuzeti vlasništvo nad svojom umjetnošću. U prošlosti rijetko koji umjetnik bio bi visoko profitabilan prodavanjem svojih umjetničkih djela jer bi često morao prepustiti dio svog vlasništva i profita platformi koja bi to djelo odlučila objaviti. Spajanje umjetnosti i blockchaina umjetnicima je omogućilo potpunu kontrolu nad njihovim umjetničkim djelima. Budući da je adresa kreatora dio metapodataka NFT-ja, prilikom svake transakcije kreator dobiva određeni postotak zarade. Također, umjetnici na taj način mogu pronaći publiku bez uključivanja platformi ili umjetničkih galerija.

Potaknute eksponencijalnim razvojem blockchain i NFT tehnologija, mnoge tvrtke odlučile su uložiti svoje resurse u izradu proizvoda virtualne stvarnosti, kao i postavljanje "metaverzuma" (engl. *metaverse*). Definicija tog pojma nije strogo definirana, već se odnosi na promjenu načina na koji komuniciramo s tehnologijom. Općenito govoreći, tehnologije na koje se tvrtke pozivaju kada govore o "metaverzumu" uključuju virtualnu stvarnost te proširenu stvarnost koja kombinira aspekte digitalnog i fizičkog svijeta.[22] Virtualna stvarnost zamišljena je kao skup virtualnih svjetova unutar kojih korisnici mogu dizajnirati svoj život, komunicirati sa stvarnim ljudima, igrati igre, kupiti virtualne nekretnine, ići na koncerte itd. NFT-jevi će služiti kao građevni blokovi "metaverzuma", to jest postat će sredstva kojima se korisnici služe u virtualnoj stvarnosti - to mogu biti kuće, ulaznice, avatari, odjeća ili jednostavno umjetnička djela koja žele pokazati drugim ljudima.[23] Daljnim razvojem tehnologije i masovnom adaptacijom koncepta "metaverzuma" polako će se brisati granica virtualnog i stvarnog svijeta, što može poboljšati neke aspekte života pojedinca, ali i uzrokovati gubljenje doticaja sa stvarnošću.

Primjena NFT tehnologije u svrhu upravljanja osobnim identitetom tek je u začetku, no ima velik potencijal u boljoj zaštiti osobnih podataka, kao i sprječavanju krađe identiteta. Krivotvorenje vozačkih dozvola, licenci, putovnica, diploma i medicinske dokumentacije samo su neki od problema koje bi eliminirali NFT-jevi. Digi-

talizacija osobnog identiteta pojedinca omogućila bi izdavanje potvrda izravno preko blockchaina kao NFT, čime bi institucije vrlo lako mogle provjeriti autentičnost vlasništva. Svaki pojedinac mogao bi vidjeti tko ima pristup njegovim podacima, kamo idu podaci te bi mogli zaraditi svaki puta kada se ti podaci prebace. Republika San Marino posvojila je ideju digitalnog dokazivanja vlasništva te je u srpnju 2021. godine uvela NFT putovnice koje dokazuju cjepljenost protiv virusa COVID-19. NFT u sebi sadržava 2 QR koda koji provjeravaju zapis o cjepljenju na VeChain blockchainu.[24] Iako digitaliziran osobni identitet sa sobom donosi brojne prednosti, postavlja se pitanje hoće li kraj online anonimnosti ugroziti našu privatnost.

3.4 Problemi

Budući da je integracija NFT-jeva u svakodnevni život tek u začetku, postoje mnogi problemi i rizici koji mogu negativno utjecati na njihovo usvajanje. Jedan od najvećih problema je stvarno posjedovanje digitalne imovine. Naime, NFT-jevi služe isključivo kao dokaz vlasništva nad imovinom, dok je stvarna imovina pohranjena na nekom od decentraliziranih sustava za dijeljenje datoteka poput IPFS-a ili središnjih poslužitelja poput AWS-a (engl. *Amazon Web Services*). Ukoliko je NFT pohranjen na centraliziranom poslužitelju, može jednostavno biti izbrisan, čak i ako je vlasnik za njega platio milijune dolara. Bezvrijednost tokena također može izazvati napad od 51% na blockchain mrežu koji bi uzrokovao poništenje transakcija.[25] Iako je vjerojatnost da će se to dogoditi na blockchainu poput Ethereuma i Cardana blizu nule, postoje centraliziraniji lanci sa slabijom sigurnosti koji mogu postati laka meta napadača.

Uz nagli porast usvajanja NFT-jeva, pojavio se znatan broj prevaranata i lažnih projekata. Najčešći tip prevare jest "povlačenje tepiha" - prevaranti koriste društvene mreže kako bi pridobili zajednicu ljudi kojima će prodavati lažna obećanja o njihovom često nepostojećem NFT projektu. Nakon što bi dobili sredstva od investitora ili ljudi koji su im vjerovali, zatvorili bi sve društvene mreže i nestali bez ikakvog traga sa dobivenim sredstvima. To je samo jedan od problema koji će se teško iskorijeniti, no na pojedincu ostaje odgovornost dobrog istraživanja projekta u koji će uložiti svoje resurse.

Poglavlje 4

Programska podrška

Prije samog razvoja aplikacije bilo je potrebno dobro razmotriti njene ciljeve kako bi se mogle odabrati odgovarajuće tehnologije koje će te ciljeve uspješno i jednostavno implementirati. Glavna svrha aplikacije jest studentima vizualno prikazati njihove dobivene studentske bedževe, tj. NFT-jeve zapisane na Ethereum ili Cardano blockchainu. Naravno, student najprije treba posjedovati studentski bedž poslan od strane Tehničkog fakulteta. Kako bi aplikacija mogla uspješno prepoznati bedževe, oni mogu biti pohranjeni na jedan od četiri kripto novčanika - Metamask, Eternl, Nami ili Flint. Metamask je danas najkorišteniji i najdokumentiraniji kripto novčanik za povezivanje sa Ethereum mrežom, stoga je očit izbor njegovog uključivanja u ovu aplikaciju. Budući da Ethereumova glavna mreža naplaćuje troškove prilikom izgradnje i testiranja aplikacije, u ovoj fazi aplikacije korištena je testna mreža Goerli. S druge strane, troškovi Cardana su neznatni, stoga je korištena glavna mreža. Odabrani su novčanici Eternl, Nami i Flint jer postoje kao proširenja web preglednika, što znatno olakšava njihovo povezivanje s aplikacijom.

Postojanje kripto novčanika u formi web proširenja jedan je od glavnih razloga zašto je ova aplikacija web, a ne mobilna. Budući da instalacija nekog od navedenih kripto novčanika dodaje novi *ethereum* ili *cardano* objekt u globalni *window* objekt, iz tog objekta jednostavno je doći do osnovnih informacija o novčaniku, kao i inicirati njegovu komunikaciju s aplikacijom. Problem mobilnih aplikacija jest u tome što one obično koriste QR kod koji kripto novčanik treba skenirati kako bi se mogao povezati s aplikacijom. Naravno, korisnik ne može skenirati QR kod na istom mobilnom ure-

đaju. Postoji nekolicina alternativnih rješenja u formi protokola koji služe kao most između kripto novčanika i decentraliziranih aplikacija, no to bi korisnika ograničilo na određeni broj novčanika koji moraju biti instalirani kao mobilne aplikacije.

Uzevši u obzir prethodno iskustvo te svrhu i opisane funkcionalnosti aplikacije, React.js nameće se kao jedna od najboljih opcija za njihovu uspješnu implementaciju. Višestruko iskoristive komponente, modularni dizajn, virtualni DOM i podrška za mnogobrojne knjižnice samo su neke od njegovih značajki koje omogućuju izradu aplikacija visokih performansi u kratkom vremenu. Iako postoje knjižnice koje omogućuju interakciju React.js-a i blockchaina, nisu se koristile prilikom razvoja ove aplikacije zbog nepotpune dokumentacije, prevelike veličine ili ograničenosti na Ethereum mrežu. Za dohvat podataka koristili su se API zahtjevi prema javnim serverima platformi Alchemy i Blockfrost, koje programerima omogućuju set razvojnih alata za komunikaciju aplikacija s Ethereum, odnosno Cardano blockchainom .

4.1 React

React.js je trenutno najpopularnija open-source knjižnica u svijetu za izgradnju web aplikacija. Povijest React-a seže do 2011. godine kada ga je stvorio Jordan Walke, softverski inženjer Facebook-a.[26] Ubrzo nakon toga korištenje React-a raslo je eksponencijalno, što dovodi do današnjih 2 milijuna aplikacija napisanih pomoću React-a.

Glavna prednost ove knjižnice jest izuzetna brzina učitavanja aplikacija. Prije Reacta, dinamičke web stranice su bile poznate po velikom kašnjenju prikazivanja podataka te je svaki gumb predstavljao novi izazov u osvježavanju korisničkog sučelja. Spora brzina učitavanja stranice bila je direktna posljedica načina na koji je internetski preglednik ažurirao Objektni model dokumenta (eng. DOM). DOM je programsko sučelje koje predstavlja web dokumente kao čvorove i objekte kako bi programski jezici mogli komunicirati sa stranicom. Najmanja promjena na jednom elementu dovodila je do toga da internetski preglednik ažurira sve komponente korisničkog sučelja, što je uzrokovalo kašnjenje. Svoju brzinu React zahvaljuje činjenici da koristi virtualni DOM umjesto stvarnog. Na taj način ažuriraju se samo objekti

koji su promijenjeni, dok ostali ostaju kakvi jesu.[27]

Također, jedno od glavnih obilježja React-a je korištenje komponenti. Komponente su neovisni i višestruko iskoristivi dijelovi koda koji mogu prihvatiti proizvoljne ulazne podatke i vraćaju React elemente koji opisuju što se treba prikazati na ekranu.[28] Unutar komponenti koristi se JSX, sintaksa Javascript-a slična XML-u koja omogućava direktno dodavanje HTML oznaka unutar Javascript-a. Na taj način komponente se odvajaju od prethodnog načina pisanja programa gdje bi se logika i HTML sintaksa odvajali u zasebne datoteke.

4.2 API pozivi

Aplikacijsko programsko sučelje (engl. *Application programming interface* - API) je sučelje koje omogućuje komunikaciju između dva programa pomoću skupa definicija i protokola.[29] Danas API-jevi čine temeljni dio web i mobilnih aplikacija jer programerima omogućuju da lako pristupe svim vrstama podataka i izbjegnu ponovnu izgradnju već postojećih značajki aplikacije.

Kako bi se uspješno mogli dohvatiti podaci o nezamjenjivim tokenima, potrebni su API pozivi. Nakon što klijentska aplikacija inicira API poziv, taj poziv dolazi do API endpoint-a na serveru gdje bude izvršen. API endpoint-ovi u ovoj aplikaciji su URL-ovi, standardizirani načini identificiranja internetskih lokacija. Svaki URL mora sadržavati protokol aplikacijskog sloja kako bi bio validan, od kojih je najkorišteniji HTTP protokol.

Za slanje asinkronih HTTP zahtjeva korištena je Axios knjižnica. Kao odgovor na zahtjev dobivaju se dva objekta: response i error. Response objekt sadrži podatke sa servera u JSON formatu, status, zaglavlja, konfiguraciju zahtjeva te XMLHttpRequest objekt. Ukoliko je došlo do pogreške u zahtjevu, error objekt uz konfiguraciju zahtjeva i XMLHttpRequest objekt vraća poruku koja opisuje pogrešku.

4.2.1 Alchemy

Alchemy je platforma koja developerima omogućuje pristup setu web3 razvojnih alata za laku izradu i skaliranje decentraliziranih aplikacija (dApp). Trenutno postoji podrška za Ethereum, Solana, Optimism, Polygon, Arbitrum, Crypto.org, Starknet i Astar mrežu, kao i njihove testne mreže.[30] Kao što je prethodno spomenuto, za potrebe aplikacije odabrana je testna mreža Goerli. Ubrzo nakon prijelaska Ethereum-a sa Proof of Work na Proof of Stake koncept u rujnu 2022. godine, Goerli testna mreža će ostati jedina podržana, dok će Rinkeby, Kovan i Ropsten testne mreže prestati biti održavane.

Za dohvaćanje svih nezamjenjivih tokena u vlasništvu određene adrese te metapodataka vezanih uz određeni nezamjenjivi token, korišten je Alchemy-ov NFT API.

4.2.2 Blockfrost

Blockfrost je API kao usluga koja korisnicima omogućuje interakciju s Cardano blockchainom i dijelovima njegovog ekosustava. Mnogobrojni API endpoint-ovi daju brz pristup podacima o Cardano mreži, računima, adresama, sredstvima, blokovima, epohama, transakcijama i tokenima. Nakon što se korisnik prijavi, dobiva jedinstveni project_id token koji se mora koristiti za autentifikaciju API poziva prema Blockfrostovom poslužitelju.

Poglavlje 5

Analiza programskog koda

Programski kod je pisan unutar Visual Studio Code (VSC) uređivača koda zbog mnogobrojnih prednosti koje pruža uključujući ugrađenu podršku za uklanjanje pogrešaka, isticanje sintakse, intuitivno korisničko sučelje, inteligentno dovršavanje koda i ugrađen Git.

React aplikacija je kreirana upisom naredbe *npx create-react-app nft-wallet* u VSC terminal, gdje je *nft-wallet* proizvoljno ime aplikacije. Naredbama *npm ime-knjižnice* instalirale su se knjižnice potrebne za ispravan rad aplikacije. *Axios* je korišten za slanje API poziva, *bech32* za enkodiranje Cardano adresa, *buffer* za upravljanje binarnim podacima, *react-icons* za dodavanje ikona, *react-router-dom* za definiranje ruta i navigaciju unutar aplikacije te *react-modal* za integraciju već gotove komponente modalnog prozora. Za definiranje stilova aplikacije korišten je stilski jezik SASS (engl. *Syntactically Awesome Style Sheets*) koji proširuje CSS (engl. *Cascading Style Sheets*) naprednim značajkama poput ugnježđivanja, varijabli i ponovo iskoristivog koda.

Polazište aplikacije je index.js datoteka unutar koje se poziva App komponenta vidljiva na slici 5.1. Funkcija svakoj komponenti aplikacije dodjeljuje njezin jedinstveni URL pomoću Route komponente iz *react-router-dom* knjižnice. Kako bi spriječili da korisnik manualno pristupi sadržaju stranica bez prethodnog spajanja novčanika, prilikom učitavanja stranice se provjerava sadržaj web pohrane (engl. *local storage*). Nakon što se korisnik spoji na Ethereum mrežu, u web pohranu se po-

hranjuje varijabla *walletAddressEth* čija je vrijednost adresa spojenog novčanika. S druge strane, ukoliko se korisnik spoji na Cardano mrežu, u web pohranu se pohranjuje njegova adresa udjela (engl. *stake address*). Istoimenim varijablama dodijeljena je njihova vrijednost iz web pohrane. Primjerice, ukoliko je varijabla *walletAddressEth* prazna, korisnik neće vidjeti sadržaj NFT galerije kao ni pojedinog tokena na Ethereum mreži.

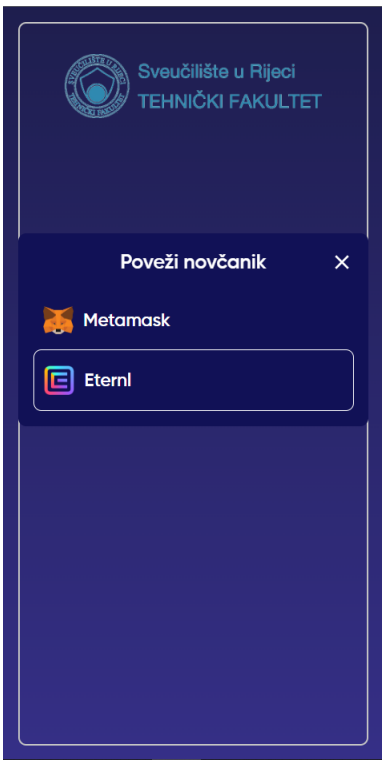
```
function App() {
  const stakeAddress = JSON.parse(localStorage.getItem("
     stakeAddress"));
  const walletAddressEth = JSON.parse(localStorage.getItem("
     walletAddressEth"));

  return (
    <div className="App">
      <Routes>
        <Route path="/" element={<Dashboard />} />
        {walletAddressEth && <Route path="nft-gallery-eth"
           element={<NFTGalleryEth />} />}
        {walletAddressEth && <Route path="nft-gallery-eth/:cid"
            element={<NFTPage/>} />}
        {stakeAddress && <Route path="nft-gallery-cardano"
           element={<NFTGalleryCardano />} />}
        {stakeAddress && <Route path="nft-gallery-cardano/:cid"
            element={<NFTPage />} />}
      </Routes>
    </div>
  );
}
```

Slika 5.1 Definiranje ruta.

5.1 Povezivanje sa kripto novčanikom

Početnu stranicu aplikacije čini jednostavno sučelje koje se sastoji od logotipa Tehničkog fakulteta te gumba *Poveži novčanik*. Klikom na gumb otvara se modalni prozor prikazan na slici 5.2. Korisniku je predstavljena opcija spajanja na Ethereum mrežu sa Metamask novčanikom ili na Cardano mrežu sa jednim od tri moguća novčanika: Eternl, Flint ili Nami. Klikom na novčanik poziva se jedna od dvije funkcije koja će spojiti aplikaciju sa Ethereum, odnosno Cardano mrežom.



Slika 5.2 Modalni prozor za povezivanje novčanika.

Popis Cardano novčanika dinamički je generiran funkcijom *checkCardanoBrowserWallets()*, prikazanom na slici 5.3. Ukoliko je neki Cardano novčanik instaliran kao web proširenje, *cardano* objekt je umetnut u *window*, globalni objekt web preglednika. Svojstva tog novčanika se zatim spremaju u objekt i dodaju u *window.cardano*. Prikazana funkcija najprije inicijalizira prazno polje *wallets*, nakon čega provjerava pos-

toji li *window.cardano* objekt. Ukoliko postoji, metodom *Object.keys()* iterira kroz objekt. Nazivima pronađenih novčanika postavlja veliko početno slovo te ih sprema u polje *wallets*. Važno je napomenuti da ukoliko je prisutan Eternl novčanik, u *window.cardano* će uz njega biti prisutan CCVault objekt, koji predstavlja njegovu raniju verziju. U tom slučaju se CCVault ne dodaje u polje.

```
const checkCardanoBrowserWallets = () => {
    const wallets = [];
    window.cardano &&
      Object.keys(window.cardano).map(function (key) {
        key !== "ccvault" &&
          wallets.push(key.charAt(0).toUpperCase() + key.slice
              (1));
      });
    return wallets;
};
```

Slika 5.3 Funkcija za traženje dostupnih Cardano novčanika.

5.1.1 Metamask

Klikom na Metamask unutar modalnog prozora poziva se funkcija *connectMetamask()* prikazana na slici 5.4. Zahtjev za povezivanjem se izvršava samo ako je unutar web preglednika prisutan *window.ethereum* objekt. Funkcija je asinkrona zbog korištenja *await* operatora koji obustavlja izvršenje dok se vraćeno obećanje zahtjeva ne ispuni ili odbije. *window.ethereum.request()* je metoda kojom korisnik šalje RPC (engl. *Remote Procedure Call*) zahtjeve Ethereum mreži putem Metamaska. Kako bi se pristupilo adresi spojenog novčanika, potrebno je specificirati metodu *eth_requestAccounts*. Dobivena adresa se zatim sprema u web pohranu kao vrijednost varijable *walletAddressEth*. Naposlijetku, korisnik je preusmjeren na stranicu koja prikazuje njegove studentske bedževe.

```
const connectMetamask = async () => {
    if (typeof window.ethereum !== "undefined") {
      const accounts = await window.ethereum.request({
        method: "eth_requestAccounts",
      });
      localStorage.setItem("walletAddressEth", JSON.stringify(
         accounts[0]));
      navigate("/nft-gallery-eth");
    }
};
```

Slika 5.4 Funkcija za povezivanje Metamaska.

5.1.2 Cardano novčanici

Klikom na jedan od Cardano novčanika poziva se asinkrona funkcija *connectCardanoWallet()* koja kao argument prima njegov naziv. Funkcija je prikazana na slici 5.5. Metoda *window.cardano.{wallet}.enable()* inicira komunikaciju s korisničkim novčanikom otvaranjem skočnog prozora koji traži dopuštenje korisnika za povezivanje s web stranicom. Ako je dopuštenje dano, API će se vratiti aplikaciji na korištenje te biti dodijeljen varijabli *api*. Ukoliko je novčanik već povezan, ova funkcija ne bi trebala zahtijevati pristup po drugi put, već samo vratiti API objekt.

Pozivom metode *getChangeAddress()* iz dobivenog API-ja, varijabli *address* pridružuje se generička adresa primanja u heksadecimalnom formatu. Adresu je potrebno enkodirati u Bech32 format kako bi adresa bila prepoznatljiva korisniku. Bech32 format implementiran je od strane Bitcoin developera kako bi smanjili pogreške prilikom slanja kriptovaluta te poboljšali korisničko iskustvo. Svaka Bech32 adresa se sastoji od proizvoljnog stringa značajnog za korisnika, separatora 1 te podatkovnog dijela koji se može sastojati od ukupno 32 mala alfanumerička znaka, isključujući broj 1 i slova 'b', 'i', 'o'. Posljednjih 6 bitova podatkovnog dijela čine

kontrolnu sumu koja djeluje kao mehanizam za uklanjanje pogrešaka.[31] Enkodiranje adrese izvršava se pozivom funkcije *bech32.encode()*.

Posljednjih 56 bitova početne adrese u heksadecimalnom formatu čine dio adrese udjela (engl. *stake address*), koja će biti potrebna prilikom slanja API zahjeva Blockfrost poslužitelju. Koristeći *bech32* knjižnicu, ovu adresu je također potrebno pretvoriti u Bech32 format.

Nakon što su obje adrese uspješno enkodirane, njihova vrijednost se pohranjuje u web pohranu kako bi im ostatak aplikacije mogao lakše pristupiti. Naposlijetku, korisnik se preusmjeruje na stranicu koja će sadržavati vizualni prikaz njegovih studentskih bedževa.

```
const connectCardanoWallet = async (wallet) => {
    try {
      const api = await eval(`window.cardano.${wallet}.enable()
         `);
      const address = await api.getChangeAddress();

      const addressEncoded = bech32.encode(
        "addr",
        bech32.toWords(Uint8Array.from(Buffer.from(address, "
           hex"))),
        1000
      );

      const stakeAddressDecoded = "e1" + address.substr(address
         .length - 56);

      const stakeAddress = bech32.encode(
        "stake",
        bech32.toWords(
          Uint8Array.from(Buffer.from(stakeAddressDecoded, "hex
             "))
        ),
        1000
```

```
      );

      localStorage.setItem("changeAddress", JSON.stringify(
         addressEncoded));
      localStorage.setItem("stakeAddress", JSON.stringify(
         stakeAddress));
      navigate("/nft-gallery-cardano");
    } catch (err) {
      console.log(err);
    }
};
```

Slika 5.5 Funkcija za povezivanje Cardano novčanika.

5.2 Dohvaćanje metapodataka sa Ethereum mreže

Nakon uspješnog povezivanja s Metamaskom poziva se komponenta zadužena za dohvaćanje metapodataka studentskih bedževa sa Ethereum mreže. Programski kod vidljiv je na slici 5.6. Prilikom inicijalnog učitavanja komponente izvršava se *useEffect* kuka (engl. *hook*). Prvi argument *useEffect*-a čini funkcija koja će se izvoditi, dok drugi argument određuje koliko često će se funkcija izvesti. U ovom primjeru drugi argument je prazno polje, koje osigurava izvođenje funkcije samo jednom kako bi se izbjegli višestruki API pozivi. Ukoliko u web pohrani vrijednost varijable *walletAddressEth* nije prazna, adresa se pohranjuje u lokalnu varijablu *walletAddress* funkcijom *setWalletAddress* koja je dio *useState* kuke. *useState* kuka kao argument prihvaća incijalno stanje i vraća dvije vrijednosti: trenutno stanje i funkciju za ažuriranje stanja. Na taj način omogućeno je održavanje stanja varijable unutar funkcijske komponente.

Nakon dohvaćanja adrese poziva se asinkrona funkcija *getMetadata* koja prima adresu kao argument. Prije slanja API zahtjeva, definiran je objekt *config* koji se

sastoji od get metode i URL-a na koji će zahtjev biti poslan. URL je definiran prema dokumentaciji Alchemy-ja i treba sadržavati API ključ generiran prilikom stvaranja novog projekta na Alchemy web stranici. Korišten API endpoint dohvaća sve NFT tokene koje sadrži navedena adresa vlasnika. Navedena konfiguracija se zatim predaje *axios()* funkciji koja kao dogvor dobiva *response* i *error* objekt. Ukoliko su podaci uspješno dohvaćeni, biti će spremljeni u polje *assetsMetadata*. Ako je došlo do pogreške, pogreška će se ispisati u web konzoli.

S obzirom da API dohvaća sve tokene trenutno pohranjene u novčaniku, tokeni se prije prikazivanja filtriraju tako da ostanu samo oni koji sadrže riječ "RiTeh" u nazivu ili opisu.

```
const [assetsMetadata, setAssetsMetadata] = useState([]);
const [walletAddress, setWalletAddress] = useState("");

// Alchemy api key
const apiKey = "HUp7fkpEemxEsjS4-nN9jy2XOP8VYSez";

const getMetadata = async (wallet) => {
    let config = {
      method: "get",
      url: `https://eth-goerli.g.alchemy.com/v2/${apiKey}/
          getNFTs/?owner=${wallet}`,
    };

    axios(config)
      .then((response) => setAssetsMetadata(response.data.
          ownedNfts))
      .catch((error) => console.log(error));
};

useEffect(() => {
    const wallet = JSON.parse(localStorage.getItem("
        walletAddressEth"));
    if (wallet !== "") {
      setWalletAddress(wallet);
```

```
      getMetadata(wallet);
    }
}, []);
```

Slika 5.6 Programski kod za dohvaćanje metapodataka sa Ethereum mreže.

5.3 Dohvaćanje metapodataka sa Cardano mreže

Nakon uspješnog spajanja korisnika sa odabranim Cardano novčanikom, pokreće se nova komponenta koja će inicirati dohvaćanje tokena. Dio programskog koda vidljiv je na slici 5.7. Slično prethodnom primjeru, na početku se samo jednom izvršava *useEffect* kuka, koja poziva asinkronu funkciju *getAssets()* ukoliko u web pohrani postoji adresa udjela.

Kako bi API poziv bio uspješan, u zaglavlje zahtjeva potrebno je dodati project_id koji je generiran prilikom stvaranja Blockfrost projekta. Project_id je spremljen u .env datoteku, gdje postaje globalna varijabla kojoj se pristupa naredbom *process.env.REACT_APP_PROJECT_ID*. URL na koji se šalje zahtjev treba sadržavati adresu udjela koja se ponovno dohvaća iz web pohrane. Ovaj API poziv razlikuje se od poziva korištenog za dohvat metapodataka sa Ethereum mreže jer vraća samo nazive tokena bez njihovih detaljnih informacija. Rezultat poziva sprema se u polje *assets* definirano *useState* kukom.

Promjena sadržaja *assets* polja rezultira pokretanjem nove *useEffect* kuke koja iterira kroz svaki prethodno dobiven token iz polja *assets* i poziva asinkronu funkciju *getMetadata()* sa nazivom tokena kao argumentom. Unutar funkcije naziv tokena se postavlja u URL kako bi se dohvatile njegove detaljne informacije. Identično prethodnom API zahtjevu, u zaglavlje je potrebno dodati projectid. Svakim API pozivom ažurira se polje *assetsMetadata* te se u njega dodaje novi objekt sa informacijama o tokenu.

Iteracijom kroz polje *assetsMetadata*, spremljeni tokeni se na prethodno opisan

način filtriraju i vizualno prikazuju na zaslonu. Kako bi se njihova slika mogla uspješno prikazati, iz URL-a slike spremljenog u objektu tokena potrebno je ekstrahirati njegov CID (engl. Content Identifier). Slike studentskih bedževa pohranjene su na IPFS preko *Pinata* servisa, stoga je potrebno dodati CID kao nastavak URL-a 'https://gateway.pinata.cloud/ipfs/'.

```
const [assets, setAssets] = useState([]);
const [assetsMetadata, setAssetsMetadata] = useState([]);

const getAssets = async () => {
    axios
      .get(
        `https://cardano-mainnet.blockfrost.io/api/v0/accounts/
           ${stakeAddress}/addresses/assets`,
        {
          headers: {
            project_id: process.env.REACT_APP_PROJECT_ID,
          },
        }
      )
      .then((res) => {
        setAssets(res.data);
      })
      .catch((error) => {
        console.error(error);
      });
};

const getMetadata = async (asset) => {
    axios
      .get(`https://cardano-mainnet.blockfrost.io/api/v0/assets
         /${asset}`, {
        headers: {
          project_id: process.env.REACT_APP_PROJECT_ID,
        },
```

```
      })
      .then((res) => {
        setAssetsMetadata((prevArray) => [...prevArray, res.
           data]);
      })
      .catch((error) => {
        console.error(error);
      });
};

useEffect(() => {
    if (stakeAddress !== "") {
      getAssets();
    }
}, []);

useEffect(() => {
    assets.map((asset) => getMetadata(asset.unit));
}, [assets]);
```

Slika 5.7 Programski kod za dohvaćanje metapodataka sa Cardano mreže.

Poglavlje 6

Testiranje aplikacije

Programski kod aplikacije javno je dostupan na Github repozitoriju, čija je poveznica `https://github.com/antoniagrabar/nft-wallet`. Nakon navigiranja u željenu mapu na lokalnom disku, u terminal se upisuje sljedeća naredba kako bi se uspješno klonirao Github repozitorij.

```
git clone https://github.com/antoniagrabar/nft-wallet.git
```

Bitno je napomenuti da se *Visual Studio Code* ovdje nameće kao jedna od najboljih opcija za kloniranje zbog ugrađenog *Git* terminala i jednostavnog pregleda dohvaćenog koda. Ulazak u novostvorenu mapu ostvaruje se naredbom

```
cd nft-wallet
```

Samo kloniranje programskog koda nije dovoljno za uspješno pokretanje aplikacije, već je potrebno instalirati sve zavisne module koji su navedeni u package.json datoteci. Procesom instalacije, moduli se preuzimaju s weba i kopiraju u mapu node_modules. Budući da se mapa node_modules može u bilo kojem trenutku stvoriti iz nule ponovnim instaliranjem modula, nepotrebno je stvaranje duplikata zbog njene opsežne veličine, kao i komplikacija prilikom nadogradnje modula na drugu verziju. Iz tog razloga mapa se ne pohranjuje na Github, već se generira naredbom

```
npm install
```

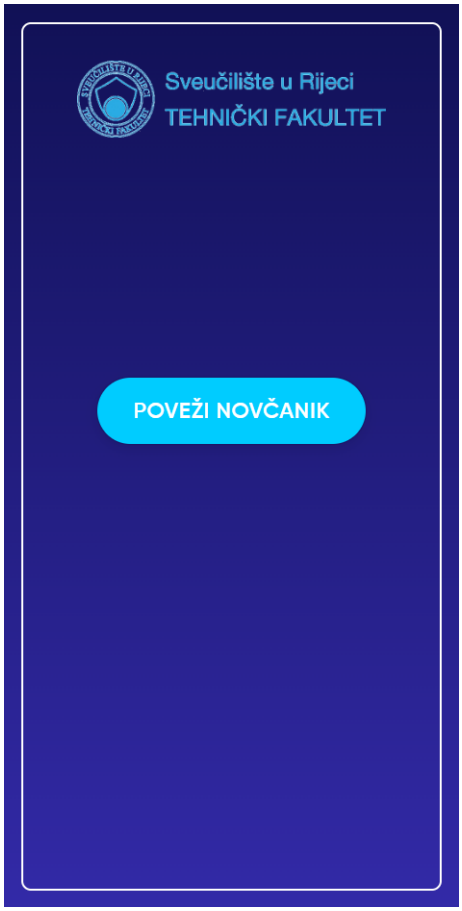
Nakon instalacije potrebnih modula, aplikacija se pokreće lokalno na portu 3000 naredbom

```
npm start
```

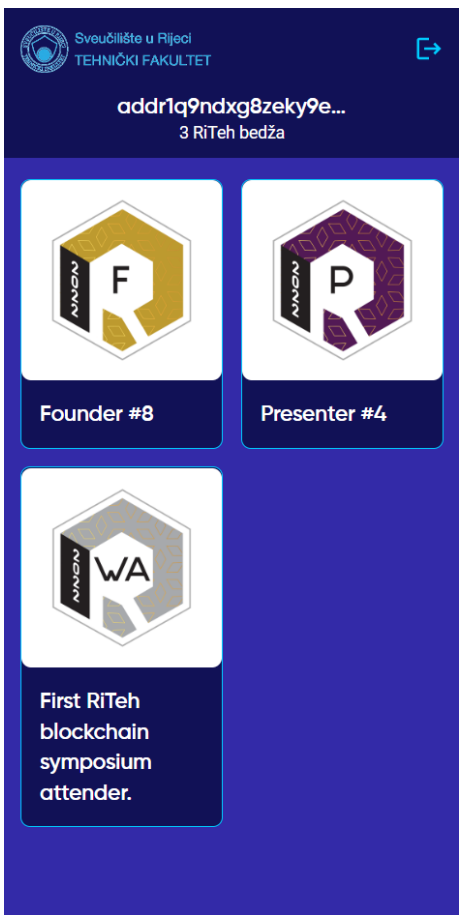
Kao što je prethodno spomenuto, pokretanjem aplikacije prikazuje se početna stranica (slika 6.1.) koja se sastoji od logotipa Tehničkog fakulteta i gumba za odabir željenog kripto novčanika. Klikom na gumb otvara se modalni prozor prethodno prikazan na slici 5.2., unutar kojeg korisnik može odabrati Metamask novčanik ili jedan od tri Cardano novčanika.

Uspješno spajanje s novčanikom korisnika dovodi do vizualnog prikaza studentskih bedževa koje posjeduje (slika 6.2.). Bitno je napomenuti da je svaki bedž predstavljen kao kartica koja prikazuje njegovu sliku i naziv, dok se klikom na bedž otvara stranica koja prikazuje detaljne informacije o samom bedžu. Na vrhu stranice nalazi se adresa spojenog novčanika te trenutni broj RiTeh bedževa u vlasništvu studenta. Također, u gornjem desnom kutu stranice nalazi se gumb za odjavu - klikom na gumb briše se sadržaj svih varijabli web pohrane te se korisnika preusmjeruje na početnu stranicu.

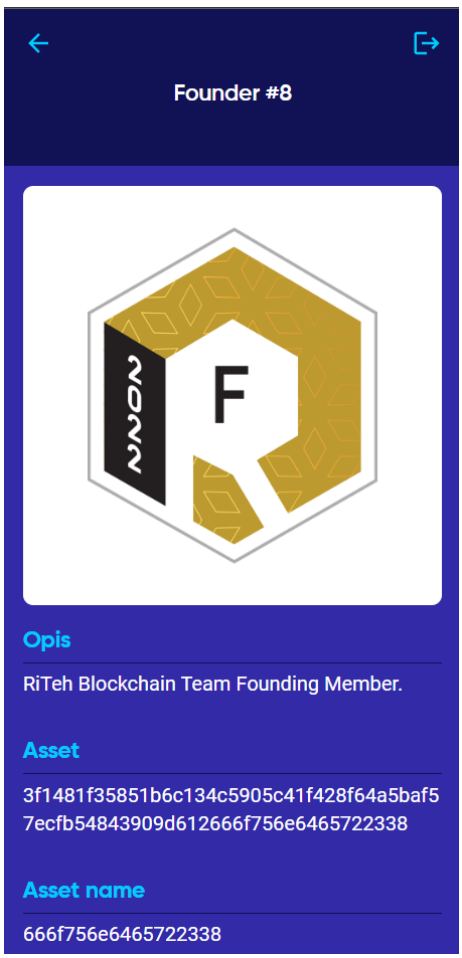
Stranica detaljnog prikaza studentskog bedža prikazuje jednostavno sučelje vidljivo na slici 6.3. U gornjem dijelu stranice nalazi se naziv bedža, gumb za povratak na prethodnu stranicu te gumb za odjavu. U sredini se nalazi uvećana slika tog bedža ispod koje su navedene dodatne informacije pohranjene na blockchainu, tj. njegovi metapodaci. Kako će se projekt studentskih bedževa dalje razvijati, mijenjat će se i prikazane informacije u skladu s proizvoljnim metapodacima zapisanima na blockchain.



Slika 6.1 Početna stranica.



Slika 6.2 Vizualni prikaz studentskih bedževa.



Slika 6.3 Detaljni prikaz studentskog bedža.

Poglavlje 7

Zaključak

Cilj ovog završnog rada bio je razviti aplikaciju gdje će studenti Tehničkog fakulteta na jednostavan način moći vidjeti dobivene bedževe te sve njihove informacije na jednom mjestu. Aplikacija je realizirana korištenjem JavaScript knjižnice React, kao i platformama Alchemy i Blockfrost koje su omogućile jednostavno dohvaćanje metapodataka sa Ethereum, odnosno Cardano mreže. Razvitak aplikacje ovdje ne staje, već se u budućnosti planira nadograditi kako bi imala više funkcionalnosti i podržavala više blockchain mreža.

Iako je razvitak NFT-jeva još u početnom stanju, uviđa se njihova velika korisnost u načinu na koji prosječna osoba može pokazati vlasništvo nad digitalnom imovinom. Digitalno vlasništvo dobiva novi sloj sigurnosti, čime bi krađa podataka mogla postati prošlost. NFT-jevi polako izlaze iz okvira umjetnosti te se proširuju na ostale sfere ljudskog djelovanja. Slično kao što je internet promijenio naše živote, danas isto čine blockchain i NFT-jevi. Budućnost NFT-jeva još je neizvjesna, no jedno je sigurno - oni su tu da ostanu zahvaljujući beskrajnim mogućnostima njihove primjene.

Bibliografija

[1] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System", 19. kolovoza 2022.

[2] A. Hayes. Blockchain Facts: What Is It, How It Works, and How It Can Be Used. , s Interneta, https://www.investopedia.com/terms/b/blockchain.asp , 19. kolovoza 2022.

[3] V. Tabora. A Decomposition Of The Bitcoin Block Header. , s Interneta, https://www.datadriveninvestor.com/2019/11/21/a-decomposition-of-the-bitcoin-block-header/ , 19. kolovoza 2022.

[4] J. Frankenfield. Consensus Mechanism (Cryptocurrency). , s Interneta, https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp , 19. kolovoza 2022.

[5] N. Reiff. How does a block chain prevent double-spending of Bitcoins?. , s Interneta, https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp, 19. kolovoza 2022.

[6] P. Wackerow. PROOF-OF-STAKE (POS). , s Interneta, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/, 21. kolovoza 2022.

[7] V. Buterin. Ethereum Whitepaper. , s Interneta, https://ethereum.org/en/whitepaper/, 21. kolovoza 2022.

[8] J. Douglas. ETHEREUM VIRTUAL MACHINE (EVM). , s Interneta, https://ethereum.org/en/developers/docs/evm/, 22. kolovoza 2022.

[9] M. Zoltu. INTRODUCTION TO SMART CONTRACTS. , s Interneta, https://ethereum.org/en/developers/docs/smart-contracts/, 22. kolovoza 2022.

[10] A. Chauhan. What Is Blockchain Oracle? , s Interneta, https://betterprogramming.pub/what-is-blockchain-oracle-ce2ad4a46c08, 23. kolovoza 2022.

[11] P. Wackerow. INTRODUCTION TO DAPPS. , s Interneta, https://ethereum.org/en/developers/docs/dapps/, 24. kolovoza 2022.

[12] The Ethereum Proof-of-Stake Merge. , s Interneta, https://ethmerge.com/, 24. kolovoza 2022.

[13] Why use Cardano?. , s Interneta, https://docs.cardano.org/new-to-cardano/why-use-cardano, 25. kolovoza 2022.

[14] Ouroboros. , s Interneta, https://cardano.org/ouroboros/, 25. kolovoza 2022.

[15] R. Sharma. Non-Fungible Token (NFT): What It Means and How It Works. , s Interneta, https://www.investopedia.com/non-fungible-tokens-nft-5115211, 27. kolovoza 2022.

[16] bit2me Academy. What is a Colored Coin?. , s Interneta, https://academy.bit2me.com/en/what-is-a-colored-coin/, 27. kolovoza 2022.

[17] V. Di Liscia. First Ever NFT" Sells for 1.4 Million. , s Interneta, https://hyperallergic.com/652671/kevin-mccoy-quantum-first-nft-created-sells-at-sothebys-for-over-one-million/, 27. kolovoza 2022.

[18] Larva Labs. CryptoPunks. , s Interneta, https://www.larvalabs.com/cryptopunks, 27. kolovoza 2022.

[19] Ethereum.org. Non-fungible tokens (NFT). , s Interneta, https://ethereum.org/en/nft/, 27. kolovoza 2022.

[20] T. Beiko. GAS AND FEES. , s Interneta, https://ethereum.org/en/developers/docs/gas/, 27. kolovoza 2022.

[21] Emurgo. Fibo 101: The 5 Unique Features of Cardano NFTs and Why They Matter. , s Interneta, https://emurgo.io/fibo-101-the-5-unique-features-of-cardano-nfts/, 29. kolovoza 2022.

[22] E. Ravenscraft. What Is the Metaverse, Exactly? , s Interneta, https://www.wired.com/story/what-is-the-metaverse/, 30. kolovoza 2022.

[23] N. S. Silver. The History And Future Of NFTs. , s Interneta, https://www.forbes.com/sites/nicolesilver/2021/11/02/the-history-and-future-of-nfts/, 30. kolovoza 2022.

[24] S. Cooling. San Marino adopts NFT vaccine passports. , s Interneta, https://finance.yahoo.com/news/san-marino-adopts-nft-vaccine-092053414.html, 30. kolovoza 2022.

[25] M. van Rijmenam. Why NFTs can be Amazing, but Not Just Yet; 5 Challenges of NFTs. , s Interneta, https://www.thedigitalspeaker.com/nfts-can-amazing-not-just-yet-5-challenges-nfts/, 30. kolovoza 2022.

[26] N. Pandit. What And Why React.js . , s Interneta, https://www.c-sharpcorner.com/article/what-and-why-reactjs/, 13. kolovoza 2022.

[27] O. Galik. When And Why You Should Use React. , s Interneta https://www.uptech.team/blog/why-use-react, 13. kolovoza 2022.

[28] Meta Platforms, Inc. Components and Props., s Interneta, https://reactjs.org/docs/components-and-props.html, 13. kolovoza 2022.

[29] Cloudfare, Inc. What is an API call?. , s Interneta, https://www.cloudflare.com/learning/security/api/what-is-api-call/, 15. kolovoza 2022.

[30] Alchemy. Alchemy API Overview. , s Interneta, https://docs.alchemy.com/reference/api-overview, 15. kolovoza 2022.

[31] L. Dashjr, J. Lau, E. Lombrozo, P. Todd. BIP 0173. , s Interneta, https://en.bitcoin.it/wiki/BIP0173, 18. kolovoza 2022.

Sažetak

U ovom završnom radu je izrađena web aplikacija za studente koristeći Ethereum i Cardano blockchain tehnologiju. Aplikacija studentima omogućuje spajanje sa njihovim kripto novčanikom te uvid u dobivene studentske bedževe, to jest nezamjenjive tokene. Kroz rad su također opisani osnovni koncepti blockchain tehnologije, kao i put nastanka te značaj nezamjenjivih tokena u dokazivanju vlasništva.

Ključne riječi — **blockchain, nft, studentski bedž, ethereum, cardano**

Abstract

In this thesis, a web application for students was created using Ethereum and Cardano blockchain technology. The application allows students to connect to their crypto wallet and view the received student badges, i.e. non-fungible tokens. The thesis also describes the basic concepts of blockchain technology, as well as the history of creation and the importance of non-fungible tokens in proving ownership.

Keywords — **blockchain, nft, student badge, ethereum, cardano**