Biometrijska autentifikacija temeljena na blockchainu

Salamon, Vito

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Diplomski studij računarstva

Diplomski rad

Biometrijska autentifikacija temeljena na blockchainu

Rijeka, svibanj 2024.

Vito Salamon
0069082515

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Diplomski studij računarstva

Diplomski rad

Biometrijska autentifikacija temeljena na blockchainu

Mentor: prof. dr. sc. Kristijan Lenac

Rijeka, svibanj 2024.

Vito Salamon
0069082515

Umjesto ove stranice umetnuti zadatak za završni ili diplomski rad

Izjava o samostalnoj izradi rada

Izjavljujem da sam samostalno izradio ovaj rad.

Rijeka, svibanj 2024.

_____

Ime Prezime

Sadržaj

Popis slika

Popis tablica

Poglavlje 1

Uvod

Blockchain i biometrija su jedne od najznačajnijih inovacija ovog doba. Blockchain tehnologija pruža nepromjenjiv i decentralizirani registar podataka s mogućnošću izvršavanja distribuiranog koda na siguran način. Korijeni Blockchaina povezani su s Bitcoin kriptovalutom čime je riješen problem dizajna distribuiranog algoritma koncenzusa o ekonomskim transakcijama bez kontrole i sudjelovanja centralnog autoriteta. Ključna, za ovaj rad, je činjenica da izuzev ekonomskih transakcija, ništa ne sprječava pohranu bilo koje druge vrste digitalnih podataka.

Povećanjem količine osjetljivih informacija pohranjenih u oblaku, raste i mogućnost digitalnih prijetnji, odnosno cyber napada. Sukladno tome, potreba za sigurnim i pouzdanim sustavima autentifikacije nikada nije bila veća.

Od svojih ranih početaka 60-ih godina do danas, ostvaren je značajan napredak u korištenju biometrije u većini svakodnevnih uređaja poput pametnih telefona. Biometrijska autentifikacija, zasnovana na jedinstvenim fizičkim(npr. lice, otisak prsta) ili ponašajnim(npr. glas, potpis) karakteristikama pojedinca, predstavlja jedan od najnaprednijih pristupa u osiguravanju autentičnosti korisnika. Glavne prednosti u odnosu na druge metode autentifikacije su uklanjanje potrebe nošenja tokena ili pamćenja lozinke te otežavanje zaobilaženja istih. Međutim, kako biometrijske informacije postaju ključne u procesu autentifikacije, njihova sigurnost i integritet postaju kritični faktori.

Biometrija je jedna od grana koja bi potencionalno mogla maksimalno iskoristiti

prednosti blockchain tehnologije. Iako su tradicionalni sustavi biometrijske autentifikacije učinkoviti, ostaje pitanje njihovih izazova što uključuje rizik curenja osjetljivih biometrijskih podataka, nedostatna pouzdanost autentifikacijskih modula te nedostatak transparentnosti upravljanja biometrijskim informacijama. Sa ciljem prevladavanja navedenih izazova, sve više istraživanja se usmjerava prema novim, inovativnim pristupima. Integracija biometrijske autentifikacije s tehnologijom blockchaina je upravo jedna od obećavajućih ideja prevazilaženja izazova tradicionalnih sustava biometrijske autentifikacije.

Ovim se radom istražuju, uspoređuju i testiraju postojeća rješenja otvorenog koda koja implementiraju biometrijsku autentifikaciju temeljenu na blockchainu. Navedeni spoj tehnologija omogućuje siguran i neporeciv način pohrane biometrijskih podataka, čineći autentifikaciju pouzdanijom. Također, omogućuje se stvaranje neovisnog traga autentifikacijskih događaja. Ipak, spoj biometrije i blockchaina nosi i potrebnu dozu opreza u očuvanju privatnosti korisnika i mogućeg curenja biometrijskih predložaka ili neovlaštenog pristupa istima. Zbog neizmjenjivosti blockchaina, moguće curenje biometrijskih podataka je teško ispraviti te može dovesti do ozbiljnih posljedica za privatnost korisnika.

Analizom postojećih rješenja istražuju se njihove prednosti, moguća poboljšanja i performanse te se žele istražiti najbolje prakse u integraciji biometrije i blockchain tehnologije.

U sljedećim poglavljima opisane su biometrija i biometrijska autentifikacija, blockchain te njegova svojstva i metode koncenzusa. U poglavlju 3. opisuje se interplanetarni datotečni sustav (IPFS) korišten za decentraliziranu pohranu podataka te pametni ugovori koji automatiziraju radnje pri izvršavanju transakcija na blockchainu. Potom, poglavlje 4. pruža osvrt na postojeća rješenja gdje su posebno analizirana tri relevantna znanstvena članka. Nakon analize postojećih rješenja, u poglavlju 5., pružen je detaljan opis provedene implementacije. Vlastita implementacija je izrađena na temelju jednog od prikazanih znanstvenih članaka te su pruženi rezultati testiranja uz bilježenje mjerenje vremena izvršavanja. Završno poglavlje pruža osvrt na obavljeni rad u sklopu izrade diplomskog rada te naglašava važnost sigurnosti, performansi i zaštite privatnosti biometrijskih podataka u sustavima koji koriste blockchain tehnologije u svrhu biometrijske autentifikacije.

Poglavlje 2

Biometrija i biometrijska autentifikacija

Biometrija kao pojam označava disciplinu koja se bavi mjerenjem i statističkom analizom fizičkih i ponašajnih karakteristika pojedinca. Biometrija se koristi u svrhe identifikacije, autentifikacije i kontrole pristupa.

Identifikacija je proces prepoznavanja pojedinca ili entiteta na temelju pruženih informacija, poput imena ili korisničkog imena, te je prvi korak u uspostavi odnosa s korisnikom. Identifikacija sama po sebi nije dovoljna za pristup sustavu ili usluzi, već zahtijeva provođenje dodatnih koraka. Verifikacija uključuje usporedbu osobnih informacija, pruženih tijekom identifikacije, s pouzdanim izvorom, poput identifikacijske isprave izdana od strane vlade, putovnice ili vozačke dozvole. Verifikacija je ključna u situacijama gdje je točnost identiteta od presudne važnosti, poput otvaranja bankovnog računa ili prijave za posao. Autentifikacija je proces potvrđivanja da je osoba ona koja tvrdi da jest. Autentifikacija je najviši stupanj jamstva identiteta i uključuje potvrdu identiteta prezentiranog tijekom verifikacije zahtijevajući da osoba pruži nešto što ima, nešto što zna ili nešto što jest. Tri vrste autentifikacijskih faktora su:

- Nešto što znate: uključuje pružanje lozinke, PIN-a ili odgovora na tajno pitanje
- Nešto što imate: uključuje prezentiranje fizičkog objekta, poput tokena, pametne kartice ili mobilnog uređaja

- Nešto što jeste: uključuje pružanje biometrijskog faktora, poput otiska prsta, prepoznavanja lica ili prepoznavanja glasa

Autentifikacija je ključna kada je sigurnost sustava ili informacija od iznimne važnosti, kao što je u online bankarstvu, medicinskim zapisima ili vladinim sustavima [1].

Biometrijska autentifikacija je konkretna primjena biometrije s ciljem potvrde identiteta. Osnovna pretpostavka biometrijske autentifikacije je da se svaka osoba može točno identificirati prema fizičkim ili ponašajnim karakteristikama [2]. Pojam biometrije potječe od grčkih riječi bio, što znači život, i metric, što znači mjeriti.

Autentifikacija korištenjem biometrije postaje sve učestalija u svakodnevnom životu. Glavni poticaj korištenja biometrije u svrhe autentifikacije, uz sigurnost, čini praktičnost pošto nema potrebe za pamćenjem lozinki ili nošenja sigurnosnih tokena.

Biometrijski identifikatori se dijele na dvije vrste, a to su fizičke i ponašajne karakteristike. Fiziološke karakteristike, koje se uobičajeno koriste u svrhu autentifikacije, čine:

- Prepoznavanje lica
- Otisci prstiju
- Geometrija prsta (veličina i položaj prstiju)
- Prepoznavanje šarenice (irisa)
- Prepoznavanje vena
- Skeniranje mrežnice (retine)
- Prepoznavanje glasa
- Podudaranje DNA (Deoksiribonukleinska kiselina)
- Digitalni potpisi

Ponašajni identifikatori obuhvaćaju jedinstvene načine na koje pojedinci djeluju. Neki od ponašajnih identifikatora mogu biti: hod, određene geste, obrasci tipkanja po tipkovnici, pokreti miša i prstiju te obrasci interakcije na web stranicama i društvenim mrežama.

2.1 Prednosti i nedostatci biometrije

Glavne prednosti korištenja biometrije:

- Teško je lažirati i/ili ukrasti biometrijske podatke, za razliku od lozinki
- Jednostavno i praktično korištenje
- Uglavnom nepromjenjivi za korisnikova života
- Neprenosivi (nontransferable) između korisnika
- Efikasnost jer predlošci (templates) zauzimaju manje prostora za pohranu

Neki od nedostataka korištenja biometrije:

- Cijena postavljanja i pokretanja biometrijskog sustava
- U slučaju da sustav ne uspije uhvatiti sve biometrijske podatke, može doći do neuspješne identifikacije korisnika
- Baze podataka koje pohranjuju biometrijske podatke su podložne hakiranju
- Moguća pojava grešaka poput lažnih odbijanja ili prihvaćanja
- U slučaju ozljede korisnika autentifikacija korisnika može biti problematična biometrijskom sustavu. Primjerice, ako korisnik opeče ruku, čitač otiska prsta možda neće moći identificirati korisnika.

2.2 Procesi biometrije

Biometrijski sustavi koriste nekoliko odvojenih procesa: upisivanje, snimanje uživo, izvlačenje predložaka i usporedba predložaka [3].

Cilj upisivanja je prikupljanje i arhiviranje biometrijskih uzoraka te generiranje numeričkih predložaka za buduće usporedbe. Čuvanjem neobrađenih uzoraka moguće je generirati nove zamjenske predloške u slučaju da se u sustav uvede nova ili ažurirana usporedna metoda. Prakse koje olakšavaju upisivanje visokokvalitetnih uzoraka ključne su za dosljednost uzoraka i poboljšavaju opću učinkovitost usklađivanja, što je posebno važno za biometrijsko identificiranje putem pretraživanja jedan

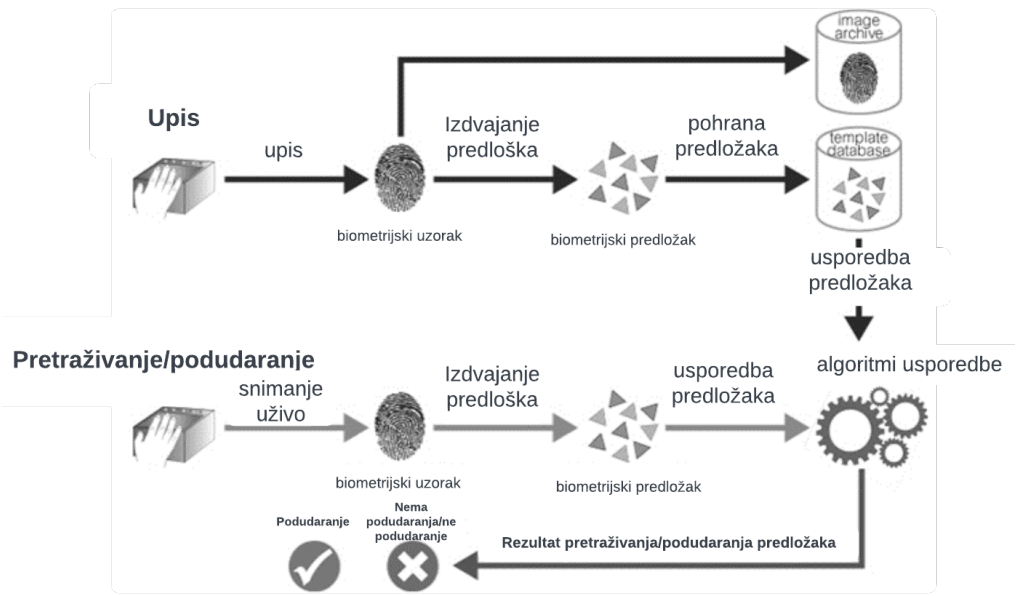
prema više.

Snimanje uživo razlikuje se od upisivanja te se definira kao proces prikupljanja biometrijskih uzoraka uživo, prilikom pokušaja pristupa ili identifikacije te usporedbe s galerijom prethodno upisanih predložaka.

Izvlačenje predložaka zahtijeva obradu signala neobrađenih biometrijskih uzoraka (primjerice slike ili zvučnih uzoraka) kako bi se dobio numerički predložak. Kako bi se uštedjelo vrijeme obrade prilikom budućih usporedbi, predlošci se obično generiraju i pohranjuju prilikom upisivanja. Procjena sličnosti biometrijskih predložaka dobiva se algoritamskim proračunima prilikom usporedbe dva biometrijska predloška. Procesom usporedbe dobivamo ukupan rezultat podudaranja. Ukoliko je rezultat podudaranja iznad određenog praga, imamo uspješno podudaranje predložaka.

Uobičajeno, algoritmi za izvlačenje i usporedbu biometrijskih predložaka su vlasnički (zaštićeni autorskim pravima, zatvorenog koda) te ih stoga nije moguće koristiti s onima drugih proizvođača u istom sustavu (primjerice, nije moguće uspoređivati predloške koje su stvorili dva različita sustava). Iznimka su MINEX certificirani generatori predložaka te algoritmi usporedbe. Navedena kategorija predložaka i algoritama podudaranja je posebno dizajnirana, testirana te neovisno certificirana kako bi bila interoperabilna za jedan na jedan provjeru što ih čini idealnima za kompaktnu pohranu na pametnim karticama ili putnim dokumentima.

Slika 2.1 prikazuje procese biometrije.



Slika 2.1 Procesi biometrije [3]

Poglavlje 3

Blockchain

Blockchain, kako samo ime sugerira, predstavlja blokove podataka povezane u neizmjenjiv, digitalni lanac [4]. Spomenuti podaci pohranjeni su u decentraliziranom okruženju otvorenog koda, u kojem je svaki podatak u bloku moguće potvrditi od strane ostalih računala prisutnih u toj sredini. Raspršena struktura poput blockchaina pomaže osigurati povjerenje, valjanost i upotrebljivost. Blockchain je konstantno razvijajuće i kompliciranо područje koje nudi sve popularniji kanal za obavljanje online transakcija i različite aplikacije.

Blokovi su registri (engl. ledgers) ispunjeni trajno zabilježenim podacima. Navedeni blokovi djeluju u distribuiranoj knjizi, što znači da se sve informacije i transakcije dijele između sudionika bez obzira na geografski položaj ili status. Knjige mogu biti otvorenog ili zatvorenog tipa, ovisno o tome tko ih ima pravo pregledavati te je li blockchain javnog ili privatnog pristupa.

Priroda decentraliziranog sustava blokova sprječava korisnike da mijenjaju podatke na blockchainu jer bi izmjena jednog djela koda odmah bila prepoznatljiva u odnosu na kopiju bilo kojeg drugog sudionika blockchaina. Sukladno navedenom, distribuirana knjiga je nepromjenjiv zapis koji je dosljedan i kronološki organiziran.

3.1 Svojstva blockchaina

U nastavku opisana su ključna svojstva blockchaina koja ga čine jedinstvenim i revolucionarnim rješenjem za razne primjene. Neka od osnovnih svojstva koja čine blockchain relevantnim za ovaj projekt:

- **Distribuiranost**: Blockchain je distribuiran sustav koji se temelji na mreži čvorova koji su raspršeni po cijelom svijetu. Svaki čvor je jednako važan, eliminirajući potrebu za centralnim autoritetima. Direktna komunikacija između čvorova (peer-to-peer; P2P) omogućava brzu i sigurnu razmjenu informacija
- **Otvorenost i pristupačnost**: Otvorenost temeljena na otvorenom kodu omogućava svima proučavanje i sudjelovanje u razvoju, dok je pristupačnost moguća s bilo kojeg mjesta u svijetu putem Interneta, čak i s pametnim telefonom
- **Neizmjenjivost i sigurnost**: Blokovi se dodaju, ali nikada ne brišu, koriste kriptografiju te su povezani u lanac. Bilo kakva promjena u nekom prethodnom bloku invalidira lanac čime se osigurava neizmjenjivost i sigurnost kompletnog sustava
- **Maksimalna redundancija i programabilnost**: Maksimalna rendancija podataka i usluga sprječava jednu točku kvara, dok je programabilnost omogućena putem tehnologija poput pametnih ugovora koji omogućavaju automatizaciju procesa
- **Samoodrživost**: sudionici su incentivinirani za sudjelovanje. Developeri su nagrađeni da razvijaju i održavaju kod, rudari da osiguravaju lanac te čvorovi da se izvršavaju i pružaju usluge. Također, pošto nitko nema root ovlasti, nitko ne može ugasiti sustav niti isključiti bilo kojeg drugog korisnika

Navedena svojstva kao posljedicu nose to da su svi podaci u blockchainu potpisani, neizmjenjivi te vremenski označeni. Osigurana je maksimalna transparentnost, odnosno odgovornost na način da je svima omogućen pregled i analiza svih zapisa. Također, eliminirana je potreba za posrednicima i centralnim tijelima te je stvoren distribuirani koncenzus za zajednički prihvat zapisa.

3.2 Blockchain izazovi

Iako je Blockchain tehnologija privukla veliku pažnju svojstvima decentraliziranosti, transparentnosti, neizmjenjivosti i ostalih, bitno je napomenuti da tehnologija nosi i neke izazove koje je potrebno razriješiti [5].

3.2.1 Skalabilnost

Jedan od problema Blockchain tehnologije je svakako skalabilnost. Blockchain mreža može biti spora i neefikasna zbog visokih računalnih zahtjeva za validaciju transakcija. S povećanjem broja korisnika, transakcija i aplikacija, smanjuje se sposobnost mreže da ih procesuira i validira na vrijeme. Navedeno čini veliko ograničenje u aplikacijama koje zahtijevaju visoke brzine obrade transakcija.

Tradicionalni blockchaini, poput Bitcoina i Ethereuma, oslanjaju se na algoritme koncenzusa poput dokaza o radu (proof-of-work) i dokaza o udjelu (proof-of-stake), koji mogu biti spori i trošiti resurse. Kao rezultat navedenoga, ove mreže imaju ograničenja propusnosti transakcija koja često dovode do zagušenja i visokih naknada transakcija.

Predložena su različita rješenja kako bi se prevladali izazovi skalabilnosti. Jedno od obećavajućih rješenja je sustav skaliranja koji omogućuje stvaranje izvanmrežnih kanala te omogućava brže i ekonomičnije transakcije. Iako postoji određeni napredak, postizanje skalabilnih i efikasnih decentraliziranih mreža ostaje neprestani izazov koji zahtijeva daljnje istraživanje.

3.2.2 Potrošnja energije

Proces validacije transakcija na blockchainu zahtijeva veliku računalnu snagu koja rezultira velikom potrošnjom energije. Sukladno navedenom, to je dovelo do zabrinutosti vezanih uz blockchain te emisije ugljika i ukupnog učinka na okoliš.

Određeni blockchain projekti su stoga počeli koristiti alternativne metode koncenzusa, poput dokaza o udjelu, koji troše znatno manje energije. Iako su dosadašnji napori smanjenja utjecaja na okoliš obećavajući, ključno je da blockchain zajednica

nastavi istraživati načine smanjenja potrošnje energije i razvoja ekološki održivih rješenja.

3.2.3 Sigurnost

Sigurnosne mjere blockchaina često su istaknute kao ključne prednosti tehnologije, no sigurnost blockchaina nije bez izazova. Zabilježeni su slučajevi sigurnosnih propusta i hakiranja mreže blockchaina. Takvi problemi mogu rezultirati gubitkom novca i ugrožavanjem integriteta mreže.

Kako bi umanjili rizike, tvrtke rade na poboljšanju blockchain mreže i aplikacija. Njihovi napori uključuju formalnu verifikaciju pametnih ugovora kako bi se identificirale potencijalne ranjivosti, kao i korištenje višestrukih potpisa za pohranu i upravljanje digitalnim sredstvima.

S nastavkom evolucije tehnologije blockchaina, osiguravanje sigurnosti korisnika, digitalnih sredstava te transakcija predstavlja i dalje jedan od najvažnijih izazova.

3.2.4 Kompleksnost

Blockchain je kompleksna tehnologija koja zahtijeva visoku razinu tehničkog predznanja za implementaciju i održavanje. Stoga, tehnički izazovi mogu predstavljati prepreku širem prihvaćanju te tehnologije, pritom odvraćajući potencijalne korisnike i developere od aktivnog sudjelovanja . Također, složenost same tehnologije može rezultirati pogreškama i neefikasnostima u implementaciji.

Kako bi se prevladali izazovi kompleksnosti razvijaju se korisnička sučelja koja olakšavaju korištenje te pojednostavljaju proces uvođenja novih korisnika. Također, važno je osigurati obuku korisnika o korištenju blockchaina te olakšati pristup obrazovnim materijalima i korisnim informacijama. Povećanje broja novih korisnika tehnologije se može potaknuti i širenjem suradnje između stručnjaka industrije, obrazovnih institucija i vladinih tijela. Takva suradnja bi mogla potaknuti dijeljenje znanja i stvaranje standardiziranih protokola i razvojnih okvira (framework) koji smanjuju prepreke ulaska novih korisnika u blockchain tehnologije.

3.2.5 Interoperabilnost

Još jedan od izazova blockchain tehnologije je interoperabilnost, odnosno sposobnost da različite blockchain mreže međusobno komuniciraju. Razvijene su brojne različite blockchain platforme koje sadrže svoje protokole i standarde, no te platforme često ne mogu zajedno funkcionirati. Nedostatak interoperabilnosti dovodi do neefikasnosti, budući da pojedinci ili tvrtke moraju navigirati kroz više platformi i koristiti različite tokene ili kriptovalute za interakciju s različitim mrežama. Također, fragmentacija može otežati suradnju, gušiti inovacije i spriječiti razmjenu podataka i vrijednosti između različitih blockchain platformi.

Razvijanje interoperabilnosti predstavlja ključ za ostvarenje punog potencijala tehnologije. Kroz razbijanje izoliranih sustava i poticanje suradnje među različitim blockchain platformama, industrija može stvoriti jedinstveno, učinkovito i pristupačno digitalno okruženje koje donosi korist korisnicima, developerima te tvrtkama.

3.3 Metode konsenzusa

Konsenzus je pojam koji označava dogovor, odnosno sporazum između korisnika decentralizirane mreže o ispravnosti podataka ili transakcija koje se nalaze u blokovima lanca. Budući da blockchain nema centralnog autoriteta koji provjerava i potvrđuje transakcije, konsenzus je ključan mehanizam koji omogućuje korisnicima mreže sporazum o tome koji su podaci valjani i trebaju biti prihvaćeni unutar blockchaina.

Dokaz o radu (Proof-of-work) i dokaz o udjelu (Proof-of-stake) su dvije najpopularnije metode obrade transakcija kriptovaluta. Iako se razlikuju po načinu izvođenja, zajednički im je cilj osigurati korisnicima da se njihove transakcije izvrše očekivano, bez problema [6].

Glavna razlika između dvije navedene metode jest ta da se metoda dokaza o radu oslanja na kripto rudarenje dok se metoda dokaza o udjelu oslanja na kripto ulog. Metoda dokaza o udjelu, omogućuje korisniku da uloži određenu svotu svojih sredstava te samim time jamči točnost novo dodanih informacija. Međutim, metoda dokaza o radu zahtijeva od korisnika rješavanje kompleksnih kriptografskih problema, što

može rezultirati značajnim energetskim troškom, prije nego što se dopusti prijedlog novog bloka.

3.3.1 Dokaz o radu

Dokaz o radu je prvi široko korišteni mehanizam konsenzusa blockchaina. Neke od popularnijih kriptovaluta koje koriste dokaz o radu uključuju Bitcoin, Litecoin i Dogecoin. Glavna značajka koja definira dokaz o radu je korištenje rudarenja, koje nagrađuje korisnike za pomoć u nadgledavanju aktivnosti na temeljnoj blockchain mreži [7].

Dokaz o radu zahtijeva od rudara da prikupe podatke o kripto transakcijama s interneta i dodaju ih u povijesni registar zapisa o vlasništvu sredstava. Međutim, prije navedenoga moraju izvršiti niz kompleksnih kriptografskih operacija dizajniranih tome da pokušaje prijevare učine skupljim. Shodno tome, rudari moraju dokazati da su obavili rad prije nego što dobe priliku predložiti novi blok transakcija.

Cijeli proces rudarenja može biti vrlo zahtijevan iz pogleda ekologije te stoga izaziva burne kritike iz sredina zabrinutih za očuvanje okoliša. Stoga, neke druge kriptovalute, poput Ethereuma, su prešle na efikasniju metodu zvanu dokaz o udjelu.

Unatoč tome, metoda dokaza o radu i dalje ostaje jedan od ključnih koncepata u svijetu kriptovaluta.

3.3.2 Dokaz o udjelu

Dokaz o udjelu je mehanizam konsenzusa dizajniran da spriječi prevare na način da plaća korisnicima da jamče svojim sredstvima legitimnost transakcija. Ulaganje je način za pasivno zarađivanje pomažući u vođenju cjelokupne blockchain mreže. Neke od popularnijih kriptovaluta koje koriste dokaz o udjelu uključuju Ethereum, Cardano, Solana i Polkadot [8].

Glavna odlika ove metode konsenzusa, u odnosu na metodu dokaza o radu, je drastična razlika u količini utrošene energije te potencijalno manja financijska barijera ulaska novih korisnika. Međutim, treba uzeti u obzir da ova metoda konsenzusa nosi

i neke rizike, poput mogućih gubitaka povezanih sa pogreškama ili prijevarama.

Ovaj mehanizam omogućava korisnicima mreže da sakupe zapise o transakcijama te ih predlože za uključivanje u trajni registar njihovog temeljnog blockchaina. Određeni korisnici, najčešće oni sa obimnim sredstvima u kriptovaluti, se mogu djelovati kao čvorovi za provjeru. Njihova računala obavljaju posao prikupljanja podataka transakcija te njihovom podnošenju za uključivanje u registar.

Navedeni validatorski čvorovi, čiji se blokovi transakcija dodaju u registar, dobivaju nagradu u obliku kriptovaluta. Stoga, postoji velika konkurencija da se postane onim čvorom čija će se informacija dodijeliti mreži. Validatori mogu povećati svoju šansu odabira na način da ulogom svojih sredstava. Ukratko, što je veći ulog to je veća šansa dobitka.

Bitno je naglasiti da u ovoj metodi postoje i rizici. Primjerice, validator može izgubiti svoj ulog u slučaju prijedloga krivih informacija ili u slučaju da računalo izgubi vezu sa mrežom.

3.4 Pametni ugovori

Pametni ugovor je program koji se samostalno izvršava te automatizira radnje potrebne u sporazumu ili ugovoru. Nakon što su dovršene, transakcije postaju praćene i neopozive.

Pametni ugovori omogućuju pouzdane transakcije i sporazume među različitim, anonimnim strankama bez potrebe za centralnim autoritetom, pravnim sustavom ili vanjskim mehanizmom provedbe.

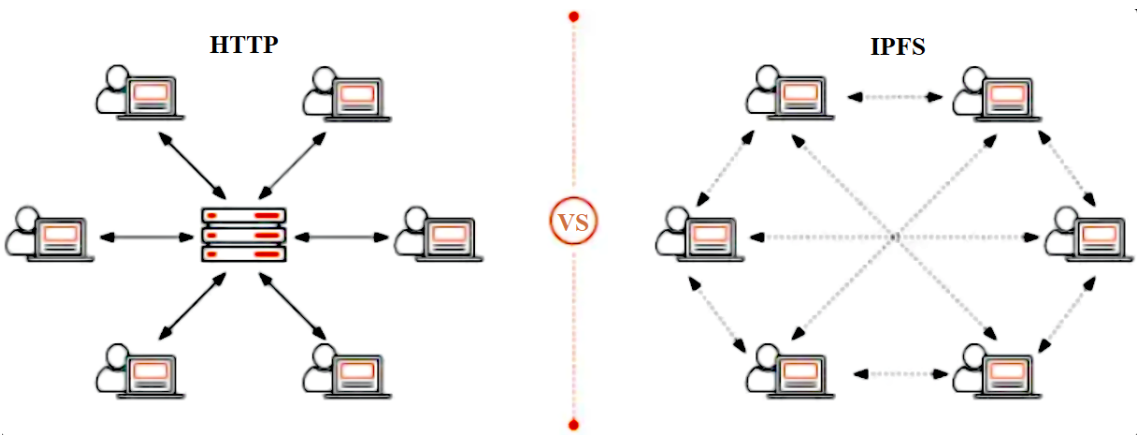
Pojam pametnih ugovora prvi put spominje 1994. godine Nick Szabo, američki računalni znanstvenik, koji je izumio virtualnu valutu „Bit Gold“ 1998. godine. Szabo je definirao pametne ugovore kao računalne protokole transakcija koji izvršavaju uvjete ugovora. Njegova ideja je bila proširiti funkcionalnosti elektroničkih metoda transakcija na digitalni svijet.

Bitno je razumjeti da pametni ugovori ne sadrže pravni jezik niti uvjete ugovora između dviju stranaka. Pametni ugovori su skripte koje sadrže if/then izjave, funk-

cije, uvoz modula i druge programske elemente koji automatiziraju radnje navedene u ugovoru [9].

3.5 IPFS

IPFS ili InterPlanetarni Datotečni Sustav je decentralizirani protokol za pohranu i dijeljenje datoteka koristeći peer-to-peer mrežu [10]. Za razliku od tradicionalnih klijent-server modela gdje su datoteke pohranjene u centraliziranom poslužitelju, IPFS omogućuje da se datoteke distribuiraju diljem mreže čvorova. Navedena činjenica, implicira da nema centralne točke kontrole i datotekama se može pristupati brže i pouzdanije. Slika 3.1 ukazuje na razliku između HTTP protokola i IPFS-a.



Slika 3.1 Usporedba HTTP protokola i IPFS-a [10]

3.5.1 Problemi centralizacije

Centralizacija često se odnosi na dominaciju velikih korporacija koje kontroliraju pristup i distribuciju informacija i usluga. To može dovesti do niza problema, poput:

- Cenzura: centralizirani entiteti imaju moć cenzurirati informacije koje smatraju neprikladnima ili štetnima, što može ograničiti slobodu govora i pristup informacijama

- Jedna točka kvara: centralizirani sustavi podložni su jednoj točki kvara. U slučaju da centralizirani entitet propadne, cijeli sustav može propasti, što može izazvati niz problema
- Ograničenje inovacija: centralizirani entiteti često imaju monopol nad informacijama i resursima, što guši konkurenciju i ograničava inovacije
- Nedostatak privatnosti: kada su podaci pohranjeni na centraliziranom mjestu, izloženiji su hakiranju i kršenju sigurnosti, što može ugroziti privatnost i sigurnost korisnika

Navedeni problemi postali su izraženiji s razvojem interneta i sve većom ovisnošću o tehnologiji u svakodnevnom životu. Decentralizacija, zajedno s korištenjem tehnologija poput IPFS-a, može pomoći u rješavanju problema centralizacije stvaranjem otvorenijeg, transparentnijeg i otpornijeg sustava.

3.5.2 Kako se pohranjuju podaci

IPFS koristi sustav adresiranja sadržaja, gdje se datoteke identificiraju jedinstvenim hash vrijednostima njihovog sadržaja, umjesto njihove lokacije ili imena. To znači da se datoteci može pristupiti i preuzeti ju s bilo kojeg čvora u mreži, bez obzira na to gdje je izvorno učitana ili pohranjena. Budući da je sadržaj adresiran, omogućuje stvaranje trajnih i nepromjenjivih veza, slično URL-ovima, koje se mogu koristiti za referenciranje datoteka čak i kada se one premještaju ili mijenjaju lokacije na mreži.

Mreža IPFS-a sastoji se od čvorova koji pohranjuju i poslužuju sadržaj. Čvorovi mogu biti pokrenuti od strane bilo koga i mogu varirati od osobnih računala do velikih podatkovnih centara. Kada čvor zatraži datoteku, šalje zahtjev za blokovima koji čine datoteku i prima ih od čvorova koji ih pohranjuju. Nakon što su svi blokovi dohvaćeni, datoteka se može rekonstruirati.

3.5.3 Prednosti IPFS-a

- Brža dostava sadržaja: IPFS može poslužiti sadržaj brže od tradicionalnih centraliziranih sustava koristeći distribuiranu mrežu čvorova te iskorištavanjem

pogodnosti peer-to-peer mreže

- Veća dostupnost podataka: mogućnost distribucije sadržaja diljem mreže čvorova pomaže povećati dostupnost podataka i smanjiti rizik od prekida rada. Čak i ako neki čvorovi postanu nedostupni, sadržaj će uvijek biti dostupan
- Poboljšana sigurnost i privatnost: kriptografske sigurnosne mjere IPFS-a osiguravaju da je sadržaj otporan na manipulaciju i dostupan samo autoriziranim korisnicima. Također, decentralizirana mreža i adresirano pohranjivanje sadržaja čine ga sigurnijim izborom od tradicionalnih centraliziranih sustava koji mogu biti podložni cenzuri i nadzoru
- Ekonomija: koristeći snagu distribuirane pohrane, IPFS može pomoći smanjiti troškove posluživanja sadržaja bez ugrožavanja brzine i sigurnosti

Poglavlje 4

Pregled postojećih rješenja

Prva faza izrade ovog diplomskog rada je posvećena istraživanju i analizi postojećih rješenja otvorenog koda za biometrijsku autentifikaciju temeljena na blockchainu.

U ovome poglavlju pruža se pregled postojećih rješenja biometrijske autentifikacije temeljena na blockchainu. S obzirom na brzi razvoj inovacija u području biometrije i blockchaina, mnogi istraživači su počeli istraživati potencijal navedene kombinacije za stvaranje sigurnih i pouzdanih sustava autentifikacije.

Danas su dostupni mnogi znanstveni radovi koji se bave analizom, implementacijom te testiranjem različitih pristupa biometrijske autentifikacije uz korištenje blockchain tehnologije. Međutim, predložene sheme ili nisu dovoljno dokumentirane ili nisu dovoljno robusne da bi se primijenile u stvarnim aplikacijama. Također, autori često podcjenjuju tehničke izazove koje stvara blockchain tehnologija ili ne raspravljaju sve aspekte problema (primjerice povjerljivost podataka predložaka).

Iako mnogi radovi pružaju dubinsku analizu te rezultate istraživanja, teško je pronaći znanstvene članke koji nude gotovu implementaciju koja je jednostavno dostupna za testiranje i uporabu što je bila prvotna ideja ovog diplomskog rada.

Nakon završetka faze istraživanja, odlučeno je pobliže analizirati tri znanstvena članka koji pružaju detaljniji opis provedene implementacije. U nastavku, u zasebnim potpoglavljima, opisani su članci "Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends" [11] i "Securing biometric authentication system using blockchain" [13].

Završni dio analize posvećen je članku "A distributed biometric authentication scheme based on blockchain" [14] jer sadrži najdetaljniji opis implementacije te primjenjuje neka od mogućih poboljšanja rješenja [11] i [13]. Upravo zbog navedenih razloga, donesena je odluka o izradi vlastite implementacije temeljene na rješenju iz članka [14].

U nastavku se pruža pregled ključnih koncepata te karakteristike različitih rješenja, ističući njihove prednosti, moguća poboljšanja i primjene.

4.1 Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends

Znanstveni članak raspravlja o izazovima u integraciji blockchaina i biometrije s naglaskom na pohranu i zaštitu biometrijskim predložaka. Rad stavlja naglasak na glavne prepreke u vezane uz navedenu integraciju poput: latencije, vremena obrade, ekonomskih troškova te performansa procesa biometrije.

U nastavku se navodi ideja, ključni zaključci, rezultati te moguća poboljšanja navedenog rješenja.

4.1.1 Implementacija

Autori članka [11] opisuju eksperimente integracije biometrije u blockchain sustavu. U svrhu istraživanja, autori proučavaju različite implementacije zaštite biometrijskih predložaka s usporedbom izvan i na lancu u Ropsten Ethereum testnoj mreži.

Člankom se razmatraju dvije različite biometrijske osobine: lice i potpis. Za lice, koriste VGG-Face model koji je jedan od najpopularnijih sustava prepoznavanja lica temeljenih na dubokim konvolucijskim neuronskim mrežama. U slučaju potpisa, koriste se varijabilne duljine predložaka koji se sastoje od ukupno 21 vremenske funkcije, izvučene iz normaliziranih X i Y prostornih koordinata kroz vrijeme.

Također, primjenjuju se tehnike zaštite biometrijskih predložaka temeljenih na biometrijskom hashiranju, koja se sastoji od konkatenacije binarnih nizova izvučenih

iz više vektorski kvantiziranih podskupova značajki s nekim stupnjem preklapanja značajki između različitih podskupova. Člankom se uspoređuju performanse zaštićenih i nezaštićenih predložaka u smislu točnosti i izračuna stope pogreške (Equal Error Rate, EER).

Uz navedeno, autori opisuju implementaciju i analizu izvedbe usporedbe na lancu temeljene na euklidskoj (nezaštićeni slučaj) te Hammingovoj udaljenosti (zaštićeni slučaj) za slučaj prepoznavanja lica. Istraživanjem je pokazano da je Hammingova udaljenost znatno jednostavnija i jeftinija za implementaciju u odnosu na euklidsku udaljenost, koja zahtijeva složene i skupe operacije s pomičnim zarezom.

Završno, autori analiziraju ekonomske troškove razmatranih shema te različitih operacija nad predlošcima (stvaranje, izmjena, brisanje te dohvaćanje i usporedba) koristeći jedinicu *gas* te američke dolare.

Gas je naknada u obliku malih dijelova kriptovalute ether (ETH) potrebna za provođenje transakcija ili izvršenje ugovora na Ethereum blockchain platformi, koja se koristi za plaćanje validatora za resurse potrebne pri transakcijama. Iznos *Gas*-a određen je ponudom, potražnjom i kapacitetom mreže u trenutku transakcije [12].

Istraživanjem je pokazano da je shema pohrane temeljena na Merkle stablima najučinkovitija i najjeftinija, jer omogućuje pohranu bilo koje količine podataka po istoj cijeni.

4.1.2 Mogućnost poboljšanja prikazane implementacije

Jedna od mogućih prilika za poboljšanje, uočena u članku [11], je u vezi s implementacijom izračuna udaljenosti biometrijskih predložaka putem pametnih ugovora. Primjena ovakve prakse može rezultirati dodatnim opterećenjem blockchain mreže te produljenjem vremena čekanja.

Pametni ugovori su osmišljeni s ciljem automatizacije i provođenja transakcija na blockchainu, te obavljaju operacije kako bi ispunili svoju svrhu. Međutim, korisnici bi trebali biti svjesni obujma operacija koje se provode unutar pametnih ugovora. U kontekstu članka, operacije izračuna udaljenosti i usporedbe biometrijskih predložaka mogu značajno usporiti obradu transakcija i povećati troškove, što predstavlja

područje za unaprjeđenje implementacije navedene sheme.

Navedeni aspekt predstavlja priliku za optimizaciju učinkovitosti i primjenjivosti u stvarnom svijetu.

4.2 Securing biometric authentication system using blockchain

Znanstveni članak [13] opisuje sustav biometrijske autentifikacije, koji koristi blockchain tehnologiju, nazvan BDAS (Blockchain-based Distributed biometric Authentication System). BDAS pruža decentralizirani i distribuirani mehanizam obrade biometrijske autentikacije te revizorski mehanizam za upravljanje biometrijskim informacijama.

Glavne značajke sustava BDAS:

- Decentralizacija i distribucija: BDAS koristi blockchain tehnologiju kako bi omogućio obradu biometrijske autentifikacije bez oslanjanja na centralni autentifikacijski modul. Svaki klijent upravlja fragmentima predložaka neovisno čime se eliminira rizik kvarova u jednoj točki
- Podjela predložaka: Svaki predložak je podijeljen na fragmente te se fragmenti čuvaju kod različitih klijenata. Segmentacija omogućuje sigurno upravljanje biometrijskim informacijama minimizirajući rizik curenja kompletnog predloška
- Transparentnost: Svaka aktivnost autentifikacije u sustavu BDAS je zabilježena kao transakcija na blockchain mreži što omogućuje praćenje autentifikacijskih aktivnosti

Ukupno gledano, BDAS poboljšava sigurnost i pouzdanost postojećih biometrijskih autentifikacijskih sustava dijeljenjem biometrijskog predloška na fragmente i njihovim upravljanjem putem blockchaina.

4.2.1 Moguća poboljšanja prikazane implementacije

U članku, autori ističu nekoliko izazova i mogućih poboljšanja za BDAS.

Moguća poboljšanja predložene sheme uključuju:

- Optimizaciju vremena autentifikacije
- Uklanjanje potrebe za većim broja sudionika blockchain mreže radi poboljšanja sigurnosti i pouzdanosti
- Upotrebu IPFS distribuiranog datotečnog sustava koja bi značajno poboljšala sigurnost cjelokupne sheme

4.3 A distributed biometric authentication scheme based on blockchain

U radu [14] predstavljena je distribuirana shema koja eliminira potrebu za centralnim čvorom koji drži biometrijske predloške korisnika kako bi se pružila što veća razina sigurnosti i zaštite informacija. Shema koristi kombinaciju Ethereum blockchaina te interplanetarnog datotečnog sustava (InterPlanetary File System, IPFS) u kojem se predlošci korisnika pohranjuju u homomorfno šifriranom obliku. Predloženo rješenje omogućuje biometrijsku autentifikaciju korisnika od strane bilo koje usluge, dok stvarni biometrijski predlošci korisnika nikada ne napuštaju njegov uređaj u nešifriranom obliku čime je osigurana sigurna autentifikacija a osjetljivi biometrijski podaci nisu izloženi nikome. Također, eksperimenti pokazuju da se shema može primijeniti kao mehanizam autentifikacije s minimalnim vremenskim preopterećenjem (overhead).

4.3.1 Općenita ideja sheme

Predložena shema pruža koncept distribuiranog mehanizma autentifikacije koji omogućuje korisnicima registraciju njihovih biometrijskih podataka te kasnije autentifikaciju. Ova shema može zamijeniti tradicionalnu infrastrukturu biometrijske auten-

tifikacije, gdje jedan čvor pohranjuje sve osjetljive biometrijske predloške te također provjerava podudaranje prilikom faze autentifikacije. Tradicionalni pristup s jednim čvorom nameće probleme koji se odnose na privatnost predložaka, valjanost dobivenih rezultata, kao i dostupnost same autentifikacijske usluge.

Glavne komponente ovog rješenja su pametni ugovori implementirani na javnoj Ethereum mreži te instanca distribuiranog IPFS datotečnog sustava. Uzima se pretpostavka da je vektor cijelih brojeva reprezentacija biometrijskih podataka korisnika, dok je odluka o autentifikaciji korisnika udaljenost između dva takva vektora. Većina shema biometrijske autentifikacije koristi navedenu pretpostavku. Rješenje se sastoji od dvije faze: faze registracije i faze autentifikacije.

Prilikom faze registracije, korisnik pomoću senzora kreira vektor biometrijskih podataka. Dobiveni vektor se potom transformira i homomorfno šifrira kroz određen broj iteracija, pritom koristeći različite parametre transformacije i različite šifrirane ključeve u svakoj iteraciji. Konačni rezultat je skup predložaka koji su različite šifrirane transformacije početnog vektora korisnika. Svaki od navedenih predložaka pohranjuje se u datoteku koja se prenosi u IPFS datotečni sustav. IPFS adrese datoteka koje sadrže predloške se potom pohranjuju u pametni ugovor Ethereum-a koji je izravno povezan s Ethereum adresom korisnika. Lokalna kopija parametara transformacije i parova šifriranih ključeva, za svaki od predložaka, je sačuvana kod korisnika te zaštićena lozinkom. Pojedini preneseni predložak se može koristiti samo jednom kako bi omogućio korisniku autentifikaciju prema usluzi treće strane. Nakon korištenja, predložak se deaktivira kako bi se smanjili pokušaji napada reprodukcijom predloška.

Prilikom faze autentifikacije, korisnik se mora autentificirati prema usluzi treće strane. Navedena usluga, nasumično odabire aktivan predložak korisnika putem pametnog ugovora, a korisnik je obaviješten o identifikatoru odabranog predloška. Korisnik potom pruža novi biometrijski vektor putem senzora. Novo stvoreni vektor se transformira i šifrira koristeći lokalno pohranjene parametre transformacije i šifrirane ključeve predloška odabranog od usluge treće strane. Vektor se zatim šalje usluzi treće strane zajedno s odabranim javnim šifriranim ključem. Potom treća strana dohvaća odabrani predložak iz IPFS datotečnog sustava i izračunava njegovu udaljenost od onoga poslanog od strane korisnika. Vektori su homomorfno šifrirani

istim ključem, pa je stoga usluzi treće strane izvedivo obaviti potrebne izračune te dobiti udaljenost u šifriranom obliku. Kako bi se donijela odluka o autentifikaciji korisnika, od korisnika se zahtijeva da dešifrira udaljenost koja je obrađena dodavanjem slučajne vrijednosti. Usluga potom donosi odluku o rezultatu autentifikacije korisnika na temelju vraćene vrijednosti.

Prilikom cijelog procesa, stvarni podaci o biometrijskom vektoru korisnika se nikad ne otkrivaju nijednoj drugoj strani osim samog korisnika. Također, podaci nisu ni pohranjeni kod korisnika već se odmah nakon proizvodnje odbacuju. Kako bi se zaštitila usluga dodaje se slučajni broj na udaljenost u posljednjem koraku autentifikacije što sprječava zlonamjernog korisnika da odgovori s narušenim odgovorom vezanim za izračunatu udaljenost.

Glavne tehnologije na kojima se bazira ova shema su Ethereum blockchain platforma, IPFS datotečni sustav te FV homomorfni algoritam šifriranja.

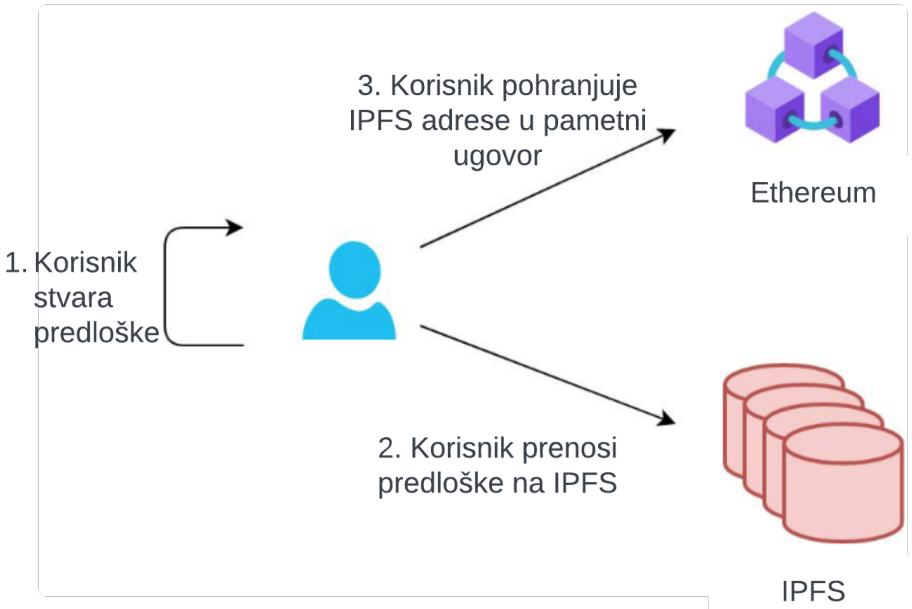
Svaki korisnik koji koristi sustav za autentifikaciju stvara skup transformiranih i šifriranih verzija početnog predloška i pohranjuje ih u IPFS datotečni sustav. Pritom, IPFS jamči dostupnost i integritet podataka pohranjenih na njemu.

Zatim korisnik implementira pametni ugovor koji pohranjuje skup parova IPFS adresa i boolean zastavica. Svaki navedeni par odgovara predlošku i označava lokaciju pohrane te njegov status (aktivan ili neaktivan). Jedini Ethereum račun koji može promijeniti stanje ugovora je njegov vlasnik koji odgovara računu korisnika. Početna procedura je prikazana na slici 4.1.

Biometrijski predlošci su homomorfno šifrirani koristeći FV enkcipcijsku shemu. Navedena shema je donekle homomorfna, što znači da omogućuje ograničenu obradu šifriranih podataka. Operacije potrebne za izračun udaljenosti dvaju vektora, u predloženoj shemi, su izvedive koristeći FV šifrirani algoritam.

4.3.2 Faza registracije korisnika

Prilikom faze registracije, korisnik registrira skup šifriranih transformiranih predložaka, generiranih iz njegovog stvarnog biometrijskog vektora, koji će se trošiti jedan po jedan tijekom njegovih pokušaja autentifikacije. Kompletan postupak možemo



Slika 4.1 Početna procedura postavljanja [14]

vidjeti na slici 4.2.

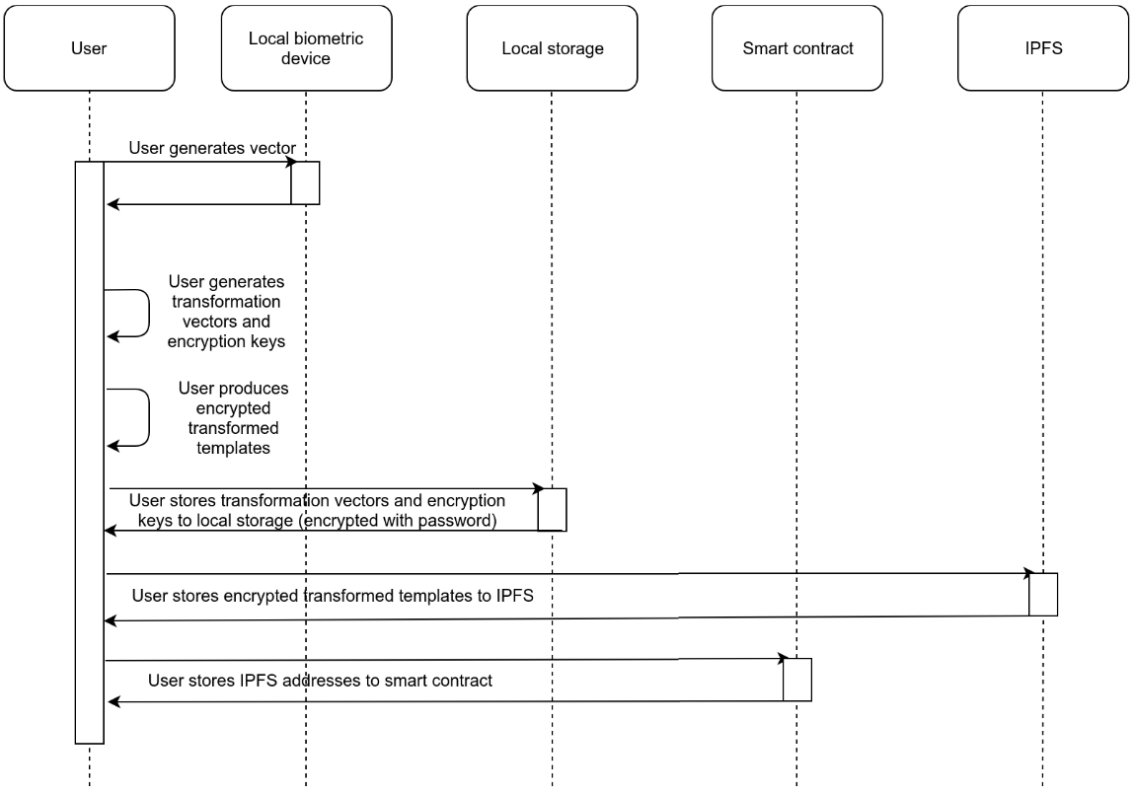
Prvi korak predstavlja korisnikovo generiranje skupa šifriranih biometrijskih vektora koji su za potrebe rada jednodimenzijski vektori cjelobrojnih vrijednosti. Uzima se pretpostavka da je X korisnikov biometrijski vektor:

$$X = [x_1, x_2, \ldots, x_n] \tag{4.1}$$

Na temelju biometrijskog vektora X generiraju se m različitih transformiranih predložaka. Navedene transformacije vođene su s m transformacijskih vektora, s jednakom duljinom izvornom biometrijskom vektoru, sastavljenih od nasumičnih cjelobrojnih vrijednosti. S obzirom da je i-ti transformacijski vektor:

$$R_i = [r_1^i, r_2^i, \ldots, r_n^i] \tag{4.2}$$

i-ti transformirani predložak će biti:



Slika 4.2 Faza registracije [14]

$$T_i = [t_1^i, t_2^i, \ldots, t_n^i] = [x_1 + r_1^i, x_2 + r_2^i, \ldots, x_n + r_n^i] \tag{4.3}$$

Generira se m parova FV šifriranih ključeva, $[(k_{\text{pub}}^1, k_{\text{pri}}^1), (k_{\text{pub}}^2, k_{\text{pri}}^2), \ldots, (k_{\text{pub}}^m, k_{\text{pri}}^m)]$ te se koriste za šifriranje svakog pojedinog transformiranog predloška. Stoga, iz i-tog transformiranog predloška T_i korisnik kreira i-ti transformirani predložak C_i koristeći k_{pub}^i ključ:

$$C_i = e_{k_{pub}^i}(T_i) \tag{4.4}$$

Svi transformacijski vektori i FV parovi ključeva su šifrirani lozinkom te su lokalno pohranjeni na strani korisnika. Od korisnika se zahtijeva korištenje iste lozinke tijekom faze autentifikacije. Konačni produkt faze registracije je set m transformi-

ranih i šifriranih predložaka $C_1, C_2, \ldots, C_n$, koji predstavljaju korisnikove predloške. Svaki od predložaka je pohranjen u datoteku, koja je potom pohranjena u IPFS datotečni sustav, te im se može pristupiti koristeći IPFS adresu koja je hash vrijednost odgovarajuće datoteke.

Korisnik stvara Ethereum pametni ugovor koji sadrži IPFS adrese m predložaka zajedno s boolean zastavicama koje označavaju je li pojedini predložak aktivan ili ne. Inicijalno su svi predlošci aktivni te se potom, kada se iskoriste u procesu autentifikacije, označavaju kao neaktivni. U bilo kojem trenutku, korisnik može ponoviti proces registracije kako bi osvježio aktivne predloške u svojem pametnom ugovoru.

4.3.3 Faza autentifikacije korisnika

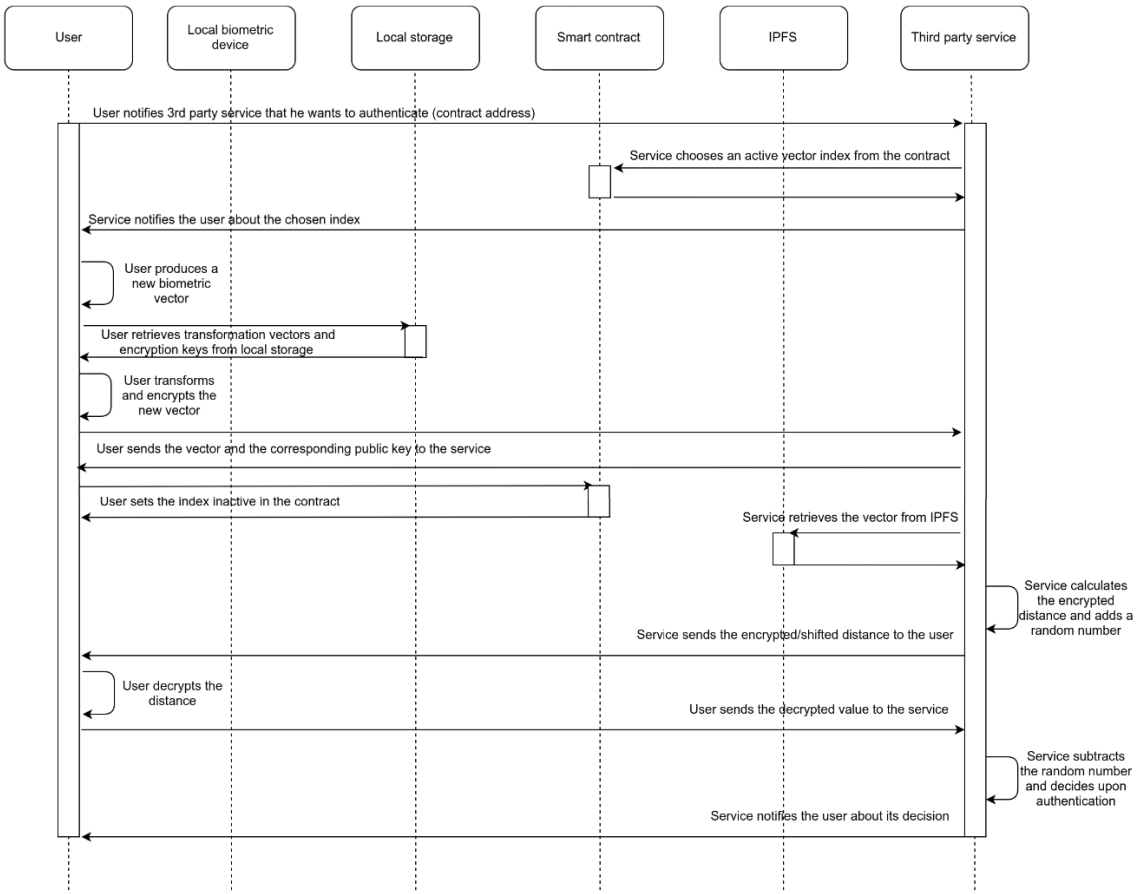
Uz pretpostavku da je korisnik već registriran te ima barem jedan aktivan biometrijski predložak, može se autentificirati prema usluzi treće strane koristeći svoje biometrijske podatke. Procedura je prikazana na slici 4.3.

Inicijalno korisnik obavijesti uslugu o adresi pametnog ugovora kojeg je implementirao. Usluga potom bira nasumični indeks j koji odgovara aktivnom vektoru iz korisnikova pametnog ugovora te obavještava korisnika o svom odabiru. Zatim, korisnik povlači odgovarajući transformacijski vektor R_j te enkripcijski par ključeva $(k^j_{\text{pub}}, k^j_{\text{pri}})$ iz svoje lokalne pohrane te ih dešifrira koristeći lozinku postavljenu prilikom registracije. Potom, korisnik generira novi biometrijski vektor Y kako bi dokazao svoj identitet. Uzimamo da je Y:

$$Y = [y_1, y_2, \ldots, y_n] \tag{4.5}$$

Korisnik koristi vraćene podatke R_j te $(k^j_{\text{pub}}, k^j_{\text{pri}})$, kako bi transformirao Y u T te kako bi šifrirao T i proizveo C. Novo proizvedeni vektor Y je transformiran i šifriran na temelju odabira nasumičnog indeksa j usluge treće strane. Navedena konstatacija znači to da je moguće usporediti stvoreni predložak C sa pohranjenim predloškom C_j.

$$T = [t_1, t_2, \ldots, t_n] = [y_1 + r^j_1, y_2 + r^j_2, \ldots, y_n + r^j_n] \tag{4.6}$$



Slika 4.3 Faza autentifikacije [14]

$$C = e_{k^j_{pub}}(T) \tag{4.7}$$

Činjenica da su rezultirajući vektor C te vektor T_j transformirani koristeći isti transformacijski vektor te šifrirani koristeći isti enkripcijski ključ, pruža mogućnost izvođenja izračuna udaljenosti između dvaju vektora. Korisnik potom šalje stvoreni vektor C zajedno sa javnim ključem k^j_{pub} usluzi treće strane. Istovremeno, korisnik mijenja stanje predloška C_j iz aktivnog u neaktivno unutar pametnog ugovora. Usluga treće strane povlači iz IPFS datotečnog sustava predložak C_j te započinje izračun udaljenosti. Pošto su dva vektora homomorfno šifrirana koristeći isti ključ, moguće je izvesti potrebne izračune. Usluga izračunava kvadrat euklidske udaljenosti dvaju vektora koristeći izraz:

$$dis(T, T_j)^2 = (t_1 - t_1^j)^2 + (t_2 - t_2^j)^2 + \ldots + (t_n - t_n^j)^2 \tag{4.8}$$

Iako usluga ima pristup samo šifriranim elementima vektora, potrebni izračuni su mogući iz razloga što su potrebne samo operacije oduzimanja i množenja za svaki od n elemenata prethodne jednadžbe te jedna operacija zbrajanja kako bi se izračunao konačni rezultat.

Povrh toga, element $t_1 - t_1^j$ nije zahvaćen transformacijom pošto je isti transformacijski vektor r_1^j iskorišten u oba slučaja. Razlika između dvaju transformiranih vektora je jednaka udaljenosti između dvaju elemenata prije transformacije. Navedeno svojstvo je prikazano izrazom:

$$t_1 - t_1^j = y_1 + r_1^j - (x_1 - r_i^j) = y_1 - x_1 \tag{4.9}$$

Sukladno navedenom, usluga računa stvarnu udaljenost dis između dvaju vektora, koristeći šifrirani oblik, pri čemu nema pristup privatnom ključu k_{pri}^j za izvođenje dešifriranja. Sljedeći korak je dodavanje nasumičnog cijelog broja r izračunatoj udaljenosti i slanje udaljenosti korisniku koji čuva privatni ključ koji omogućava dešifriranje. Homomorfna svojstva FV algoritma omogućavaju dodavanje nešifriranog broja r šifriranoj udaljenosti $(T, T_j)^2$.

Korisnik prima vrijednost dis + r u šifiranom obliku, podatak dešifrira te ga šalje natrag usluzi treće strane. Usluga potom oduzima nasumičnu vrijednost r iz vraćene vrijednosti te dobiva stvarnu udaljenost između dvaju vektora u nešifriranom obliku. Konačno, usluga može donijeti autentifikacijsku odluku o korisnikovom pokušaju autentifikacije temeljem vrijednosti udaljenosti. Nasumična vrijednost r omogućava usluzi zaštitu od korisnika da ne izmjenjuje povratnu dešifriranu vrijednost sukladno njegovoj namjeri. Korisnik nije svjestan stvarne vrijednosti koja odgovara udaljenosti dvaju vektora čime se sprječava izmjena vrijednosti te prisilna uspješna autentifikacija.

4.3.4 Izvorna implementacija

Autori su razvili prototipnu implementaciju predložene sheme kako bi kako bi potvrdili njezinu funkcionalnost. Iako je sustav osmišljen za implementaciju na javnom blockchainu te javnoj distribuiranoj mreži za pohranu, koncept je implementiran na eksperimentalnoj privatnoj instalaciji kako bi se provjerila predložena shema. Glavni dio eksperimentalne implementacije čine privatna Ethereum mreža, privatna IPFS mreža, implementacija korisnika te implementacija usluge.

Za Ethereum mrežu, instaliran je geth klijent na tri čvora te su sve instance konfigurirane da tvore malu privatnu Ethereum mrežu. Navedeno se potom koristi kako bi korisnik implementirao pametni ugovor. Za IPFS mrežu, koriste se ista tri čvora te je instaliran set od tri IPFS klijenta. Navedeni klijenti formiraju distribuirani datotečni sustav koji pruža osnovu za pohranu šifriranih i transformiranih predložaka.

Što se tiče klijentske implementacije, napravljena je docker slika koja sadrži potrebne knjižnice (Microsoft PySeal implementacija FV algoritma, web3 knjižnica za pristupanje ethereum pametnim ugovorima te ipfsapi knjižnica za komunikaciju s IPFS datotečnim sustavom). Navedena docker slika sadrži sve razvijene funkcionalnosti vezane uz registraciju te autentifikaciju.

U konačnici, za implementaciju usluge je također razvijena slična docker slika koja uključuje iste knjižnice kao i klijentska slika zajedno s funkcionalnošću razvijenom za uslužnu stranu.

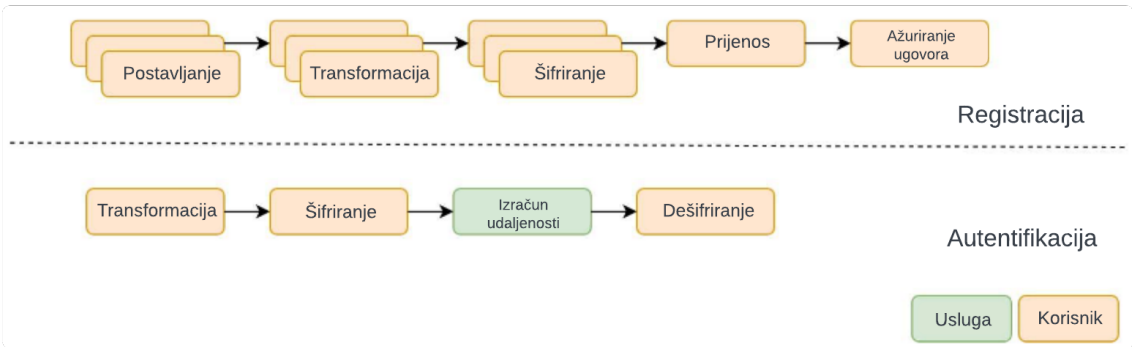
4.3.5 Dobiveni rezultati istraživanja

Glavne operacije koje sustav provodi:

- Postavljanje: inicijalno postavljanje FV algoritma te generiranje ključeva za svaki od predložaka
- Transformacija: transformacija predloška za svaki od predložaka
- Šifriranje: šifriranje predloška se izvršava za svaki od predložaka
- Prijenos: prijenos predložaka na IPFS koji se događa jednom za sve predloške

- Ažuriranje ugovora: ažuriranje pametnih ugovora sa IPFS adresama koje se događa jednom za sve predloške
- Računanje udaljenost: računanje udaljenosti se izvršava na serverskoj strani te se događa jednom za svaki pokušaj autentifikacije
- Dešifriranje: dešifriranje udaljenosti na klijentskoj strani se događa jednom za svaki autentifikacijski pokušaj

Navedene operacije su prikazane slikom 4.4 u odnosu na dvije glavne faze ove sheme, fazu registracije te fazu autentifikacije



Slika 4.4 Operacije u pojedinim fazama izvođenja [14]

Faza registracije se provodi na klijentskoj strani. Postavljanje, transformacija i šifriranje su operacije koje se događaju jednom za svaki proizvedeni predložak, dok se prijenos i ažuriranje ugovora događaju jednom za cijeli set predložaka. Za fazu autentifikacije pojedinačne instance transformacije i šifriranja događaju se na klijentskoj strani, potom usluga provodi operaciju izračuna udaljenosti te na kraju klijent provodi jednu operaciju dešifriranja.

Kako bi procijenili aspekt performansi, autori predložene sheme su proveli testiranje te analizirali vrijeme potrebno za zaključenje cijelog postupka s obzirom na razinu sigurnosti koju pruža FV algoritam. Glavni konfiguracijski parametar je polinomni modul, čija vrijednost se vrijednost kretala između 1024, 2048, 4096, 8192, 16384, 32768. Autori su proveli testiranje na prosječnom osobnom računalu te su korišteni vektorski predlošci duljine 10. Rezultati istraživanja su prikazani u tablici

4.1.

Tablica 4.1 Trajanje operacija (u sekundama) za različite polinomne module [14]

Operacija	**Polinomni modul**					
	1024	**2048**	**4096**	**8192**	**16384**	**32768**
Postavljanje	0,0219	0,043	0,078	0,149	0,287	0,577
Transformacija	0,001					
Šifriranje	0,0658	0,123	0,240	0,472	0,953	1,951
Prijenos	ovisi o IPFS mreži					
Ažuriranje	ovisi o Ethereum mreži					
Izračun	0,0890	0,165	0,328	0,667	1,404	2,755
Dešifriranje	0,0123	0,025	0,053	0,101	0,193	0,396

Glavni zaključci iz niza eksperimenata su da, na prosječnom osobnom računalu i za relativno sigurnu opciju iz pogleda polinomnog faktora, korisnik može pripremiti biometrijski predložak s zadovoljavajućom brzinom. Koristeći polinomni faktor 4096, priprema predloška zahtijeva 0.078+0.001+0.240=0.339 sekundi. Sukladno tome, korisnik može pripremiti 100 predložaka u približno 30 sekundi.

Prijenos predložaka na IPFS datotečni sustav te ažuriranje pametnih ugovora su operacije koje ovise o postavkama korisnikove mreže. U općem slučaju, očekivano je da korisnik može pripremiti i postaviti 100 predložaka u manje od minute.

Što se tiče faze autentifikacije, uzimajući u obzir isti hardver, operacije koje je potrebno izvršiti su: transformacija, šifriranje predloška, izračun udaljenosti te šifriranje dobivene udaljenosti. Izvršavanje navedenih koraka iznosi: 0.001 + 0.240 + 0.328 + 0.053 = 0.622 sekundi. Također, bitno je uzeti u obzir i dodatni trošak mrežne komunikacije između korisnika i usluge, no sveukupno kašnjenje od 0.6 sekundi, koje izaziva faza autentifikacije predložene sheme, je nisko u odnosu na trajanje tradicionalnog procesa autentifikacije.

U slučaju korištenja navedene sheme u javnoj mreži, potrebno je uzeti u obzir još neke parametre. Javni IPFS datotečni sustav kreira dodatni mrežni trošak, dok korištenje javne Ethereum mreže može izazvati dugotrajna kašnjenja s obzirom na čekanje potvrde transakcija. Početno generiranje i prijenos predložaka zahtijeva prijenos više datoteka na IPFS, zajedno s nizom transakcija na Ethereum mreži. Cijeli postupak može biti dugotrajan te ovisi o mnogo različitih čimbenika. Međutim,

cijeli postupak se može odvijati asinkrono za korisnika. Korisnik može pokrenuti postupak, stvoriti početni predložak, a zatim uređaj nastavlja s ostatkom postupka te obavještava korisnika kada je postupak gotov. Uzevši u obzir korisničko iskustvo, ovakav pristup je prihvatljiv. Prilikom svakog pokušaja registracije, usluzi treće strane mora pročitati datoteku s IPFS datotečnog sustava te pozvati funkciju pregleda na Ethereum pametnom ugovoru. Spomenute radnje ne izazivaju kašnjenja u cijelom postupku. Korisnikov uređaj mora ažurirati oznaku aktivnosti za korišteni biometrijski predložak koristeći pametni ugovor, što može potrajati, no ta se akcija provodi asinkorno u odnosu na autentifikaciju tako da ne utječe na sveukupno korisničko iskustvo.

4.3.6 Zaključak istraživanja

Autori su implementirali prototip predloženog sustava kako bi potvrdili njegovu funkcionalnost. Rezultati istraživanja pokazali su da sustav omogućuje korisniku točnu i pravovremenu autentifikaciju, bez potrebe za pouzdanim rješenjima treće strane koje bi pohranjivale i upravljale biometrijskim predlošcima.

Stvarni scenarij uporabe predloženog sustava mogao bi biti nosivi uređaj za otiske prstiju. Korisnik na početku postavlja uređaj te stvara svoj početni set šifriranih i transformiranih vektora. Kad god se korisnik treba autentificirati prema usluzi treće strane, fizički bliskoj ili udaljenoj, tada se izvršavaju sljedeći koraci:

1. Usluga treće strane zahtijeva adresu pametnog ugovora od nosivog uređaja
2. Usluga obavještava nosivi uređaj o odabranom ID-u biometrijskog predloška
3. Korisnik koristi senzor uređaja i ID kako bi stvorio novi vektor
4. Usluga sigurno izračunava udaljenost i odlučuje je li korisnik povezan s ugovorom ili ne

Biometrijski predlošci korisnika pohranjeni su na IPFS mrežu za pohranu samo u transformiranom i šifriranom obliku. Čak i u slučaju da zlonamjerni korisnik uspije dešifirati vektor predloška, ne može zaključiti stvarni biometrijski vektor koji je korisnik koristio prilikom faze registracije, jer je taj vektor nasumično transformiran.

Jedini slučaj u kojem zlonamjerni korisnik može koristiti predložak kako bi dobio stvarni biometrijski vektor je da posjeduje privatni ključ za šifriranje i vektor transformacije. Navedene informacije nikada se ne prenose nikome te ostaju na uređaju korisnika. Također, navedene informacije su šifrirane koristeći lozinku, na uređaju korisnika, tako da i u slučaju krađe uređaja nitko nema pristup stvarnim podacima.

Kako bi se netko uspješno autentificirao, trebao bi imati stvarni biometrijski vektor te parametre transformacije i enkripcije proizvedene tijekom registracije, što je vrlo teško postići zlonamjernom korisniku.

Predloženi sustav omogućuje sigurnu i privatnu biometrijsku autentifikaciju korisnika.

Poglavlje 5

Vlastita implementacija biometrijske autentifikacije

U sklopu izrade diplomskog rada, donesena je odluka izrade vlastitog rješenje temeljenog na članku [14]. Koncept korištene sheme biometrijske autentifikacije temeljenoj na blockchainu iz članka detaljno je objašnjen u prethodnom poglavlju.

Glavna ideja članka je zadržana te se prilikom izrade pokušala napraviti vjerna kopija originalne ideje. Međutim, treba imati u vidu da su neke stvari napravljene drukčije te neke stvari nisu implementirane u konačnom rješenju.

Jedna od ključnih razlika između naše implementacije i originalnog članka leži u načinu na koji su mreže i komponente modelirane. U originalnom članku, autori koriste tri klijenta koji čine privatnu Ethereum mrežu te tri klijenta koji čine IPFS mrežu, uz korištenje dva Docker kontejnera koji su simulirali klijenta i uslugu treće strane.

Vlastita implementacija koristi Ganache razvojnu Ethereum mrežu, dok je za potrebe IPFS-a korišten jedan IPFS klijent koji se spaja na javnu IPFS mrežu. Uz navedeno, klijent i usluga treće strane simulirani su korištenjem jedne konzole Python aplikacije. Takva prilagodba omogućava jednostavniju upotrebu i testiranje naše implementacije te smanjenje složenosti konfiguracije.

Još jedna razlika je, u koraku registracije, nedostatak kreiranja višestrukih biometrijskih predložaka radi pojednostavljenja konačnog rješenja. Unatoč nedostatku,

implementacija ove funkcionalnosti bi poboljšala sigurnost biometrijskih predložaka. Pri izradi, veći naglasak je stavljen na osiguranje funkcionalne komunikacije između svih komponenti sustava te njihovo uključivanje u konačno rješenje.

Sukladno navedenom, važno je napomenuti da se, zbog različitih pristupa, rezultati testiranja našeg rješenja mogu razlikovati od onih prikazanih u znanstvenom članku.

5.1 Korišteni alati

Programsko rješenje je temeljeno na programskom jeziku *Python*, koji je korišten zbog široke rasprostranjenosti, jednostavnosti korištenja te velikog broja dostupnih knjižnica funkcija. Također, uz osnovne jezične funkcionalnosti, koriste se različite Python biblioteke koje olakšavaju razvoj i implementaciju.

Konkretno, za komunikaciju s IPFS mrežom je korištena knjižnica *ipfshttpclient* [15], za manipulaciju podacima i matematičke operacije korištena je knjižnica *numpy* [16] te je korištena knjižnica *getpass* [17] za sigurno i povjerljivo unošenje lozinki. Uz navedene, korištena je ugrađena knjižnica *json* [18] za serijalizaciju i deserijalizaciju podataka, modul *time* [19] za provođenje mjerenja vremenskih performansi izvođenja, modul *os* [20] za interakciju s operativnim sustavom te *web3* [21] knjižnica za interakciju s Ethereum mrežom.

Temelj cijelog rješenja predstavlja *Microsoft SEAL* knjižnica [22], koja se koristi za homomorfnu enkripciju. Homomorfna enkripcija je ključna tehnika koja omogućava izvođenje operacija nad šifriranim podacima, čime se osigurava privatnost i sigurnost podataka čak i prilikom izvođenja računalnih operacija. Za integraciju s programskih jezikom *Python*, korištena je *SEAL – Python* wrapper knjižnica [23], koja pruža sučelje za korištenje *Microsoft SEAL* knjižnice u *Python* okruženju.

Slijedeću komponentu programskog rješenja čini desktop aplikacija *Ganache* [24]. *Ganache* se koristi za postavljanje Ethereum razvojne mreže u kojoj možemo raditi razvoj pametnih ugovora, aplikacija te provođenje testova. Jedna od ključnih prednosti korištenja *Ganache*-a je u tome što nam omogućava da izvodimo sve akcije dostupne i na javnoj blockchain mreži, bez potrebe za stvarnim ulaganjima ili troše-

njem vlastitih resursa. Također, *Ganache* omogućava brzo i jednostavno testiranje funkcionalnosti pomoću trenutačnog rudarenja blokova što znači da nismo ograničeni čekanjem glavne mreže da izrudari traženi blok. Pri razvoju aplikacija možemo koristiti tri okruženja blockchaina tehnologija:

- Mainnet: glavna mreža u blockchainu, u kojoj se odvijaju stvarne transakcije i u kojoj kriptovalute imaju stvarnu vrijednost
- Devnet: razvojna mreža koja se koristi za razvoj i testiranje aplikacija prije nego što se one prebace na mainnet. Ovdje se mogu isprobavati nove funkcionalnosti, alati i softveri bez rizika stvarnih troškova
- Testnet: testna mreža s fokusom na simulaciju stvarnih uvjeta mainneta, ali se koristi za testiranje i eksperimentiranje s novim softverom, bez rizika gubitka stvarnih sredstava. Testnet kriptovalute nemaju stvarnu vrijednost te se mogu dobiti besplatno izrađivanjem zahtjeva. Ovo je korisno za programere i korisnike koji žele testirati svoje aplikacije prije lansiranja na mainnet.

Još jedna od potrebnih komponenti je *Remix IDE* [25] koji se temelji na web pregledniku te omogućava pisanje pametnih ugovora koristeći Solidity programski jezik. *Remix IDE* je široko korištena platforma u blockchain zajednici zbog jednostavnosti korištenja i bogatog skupa značajki. Osim što omogućava pisanje pametnih ugovora, *Remix IDE* pruža napredne mogućnosti testiranja i otklanjanja grešaka. Integrirani alati za testiranje olakšavaju provjeru ispravnosti pametnih ugovora prije njihove implementacije na stvarnu ili testnu Ethereum mrežu. Uz navedeno *Remix IDE* pruža i materijale za učenje koji omogućavaju programerima da brzo savladaju *Solidity*.

Konačno, zadnju komponentu čini *IPFS Desktop* aplikacija [26] koja pakira IPFS čvor, upravitelj datoteka i čvorova te istraživač sadržaja u jednu intuitivnu aplikaciju. *IPFS Desktop* aplikacija omogućava jednostavno upravljanje IPFS mrežom bez potrebe korištenja naredbenog retka.

5.2 Rješenje

U ovom poglavlju detaljno ćemo istražiti programsko rješenje koje je razvijeno koristeći Python programski jezik, pri čemu se koristi naredbeni redak ako sučelje kojim korisnik komunicira s aplikacijom. Izrađena aplikacija predstavlja sveobuhvatno rješenje koje se sastoji od dvije faze: registracije i autentifikacije. Kroz ova dva koraka, korisnicima se pruža siguran i intuitivan način za registraciju i provjeru autentičnosti, pri čemu se osigurava pouzdana zaštita njihovih podataka.

5.2.1 Faza registracije

Prvu fazu čini registracija korisnika. Prilikom registracije, korisniku se pruža mogućnost korištenja odluke kao postojeći korisnik ili vršenja nove registracije.

Ovisno o odluci aplikacija se kreće u jednom od dva smjera. Ukoliko se radi o novom korisniku, od korisnika se traži unos imena i lozinke. Nakon unosa imena i lozinke, od korisnika se traži skeniranje, odnosno pružanje svog biometrijskog predloška. Nakon pružanja potrebnih podataka, aplikacija generira privatni i javni ključ korisnika koristeći Brakerski/Fan-Vercauteren (BFV) enkripcijsku shemu. Slijedi generiranje transformacijskog vektora. Transformacijski vektor nastaje generiranjem liste, dužine jednake originalnom biometrijskom predlošku, nasumičnih cjelobrojnih vrijednosti. Potom se postupak nastavlja transformacijom originalnog predloška na način da se svakom članu originalnog biometrijskog predloška pribroji pripadajući član transformacijskog vektora. Nakon transformacije, biometrijski predložak se šifrira koristeći SEAL-ove funkcije šifriranja. Postupak se privodi kraju prijenosom šifriranog predloška na IPFS čime se dobiva hash kreirane datoteke koji će se koristiti u fazi autentifikacije. Konačno, postupak se završava izvršavanjem pametnog ugovora koji radi javljanje registriranog korisnika.

Ukoliko je korisnik već registriran, korisnik radi odabir između već registriranih korisnika. Nakon odabira odgovarajućeg korisnika, korisnik je zamoljen za unos lozinke te, ako je lozinka ispravna, postupak se nastavlja dohvaćanjem svih potrebnih podataka za daljnji proces. Sukladno navedenom, dohvaćaju se privatni i javni ključ korisnika te transformacijski vektor lokalno pohranjeni na strani korisnika. Također,

dohvaća se šifrirani biometrijski predložak sa IPFS-a koristeći hash dobiven prilikom prvotne registracije korisnika, odnosno njegova uvođenja u sustav. Dohvaćanjem potrebnih podataka, završava se postupak registracije postojećeg korisnika.

Kompletan slijed izvođenja faze registracije je moguće vidjeti na slici 5.1 gdje je prikazan kompletan proces izvođenja dijagramom toka.

5.2.2 Faza autentifikacije

Faza autentifikacije započinje unosom lozinke. Ukoliko je lozinka ispravna, korisniku se pruža mogućnost odabira između četiri predefinirana izbora korisnička predloška za autentifikaciju ili vršenja novog skeniranja, odnosno unošenja novog biometrijskog predloška. Potom se dohvaćaju svi potrebni podaci korisnika.

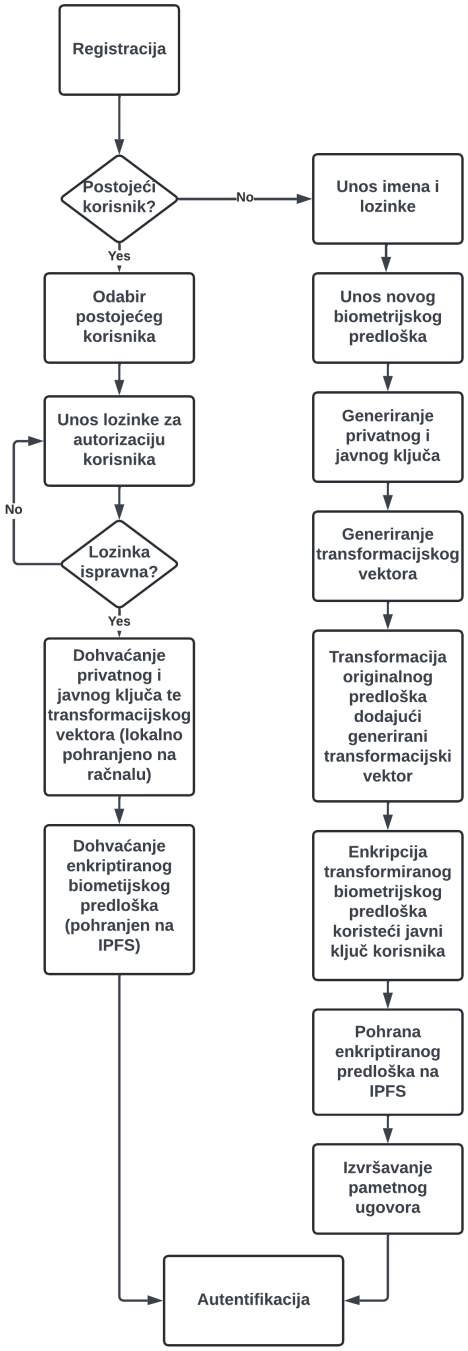
Sukladno navedenom, dohvaćaju se privatni i javni ključ korisnika te transformacijski vektor lokalno pohranjeni na strani korisnika. Također, dohvaća se šifrirani biometrijski predložak sa IPFS-a koristeći hash dobiven prilikom prvotne registracije korisnika, odnosno njegova uvođenja u sustav.

Postupak se nastavlja transformacijom novog biometrijskog predloška koristeći originalni transformacijski vektor stvoren u procesu registracije trenutnog korisnika. Novi transformirani biometrijski vektor se zatim šifrira koristeći javni ključ korisnika. Potom se vrši izračun euklidske udaljenosti homomorfno šifriranih biometrijskih vektora.

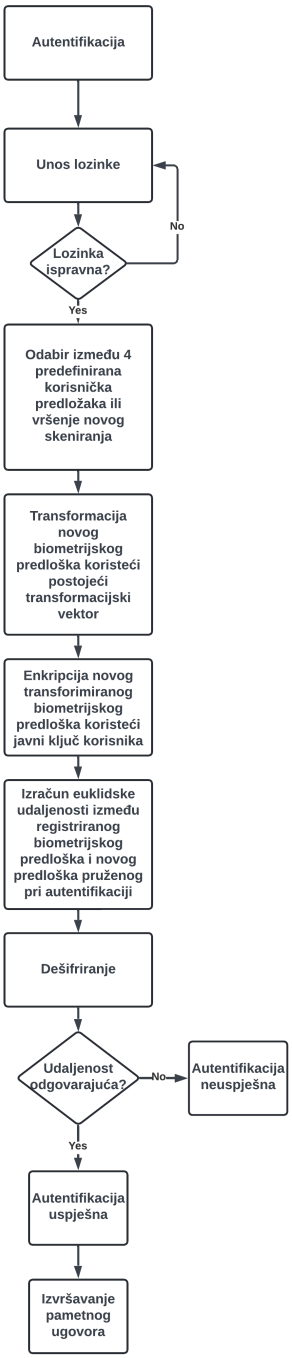
Ovisno o izračunatoj udaljenosti donosi se odluka o autentifikaciji korisnika, odnosno ako je udaljenost manja od unaprijed definiranog praga korisnik je uspješno autentificiran. U radu, prag je postavljen na vrijednost 0.1.

Postupak završava izvođenjem pametnog ugovora kojim se ispisuje poruka autentifikacije trenutnog korisnika.

Kompletan slijed izvođenja faze autentifikacije je moguće vidjeti na slici 5.2 gdje je prikazan kompletan proces izvođenja dijagramom toka.



Slika 5.1 Faza registracije - dijagram toka

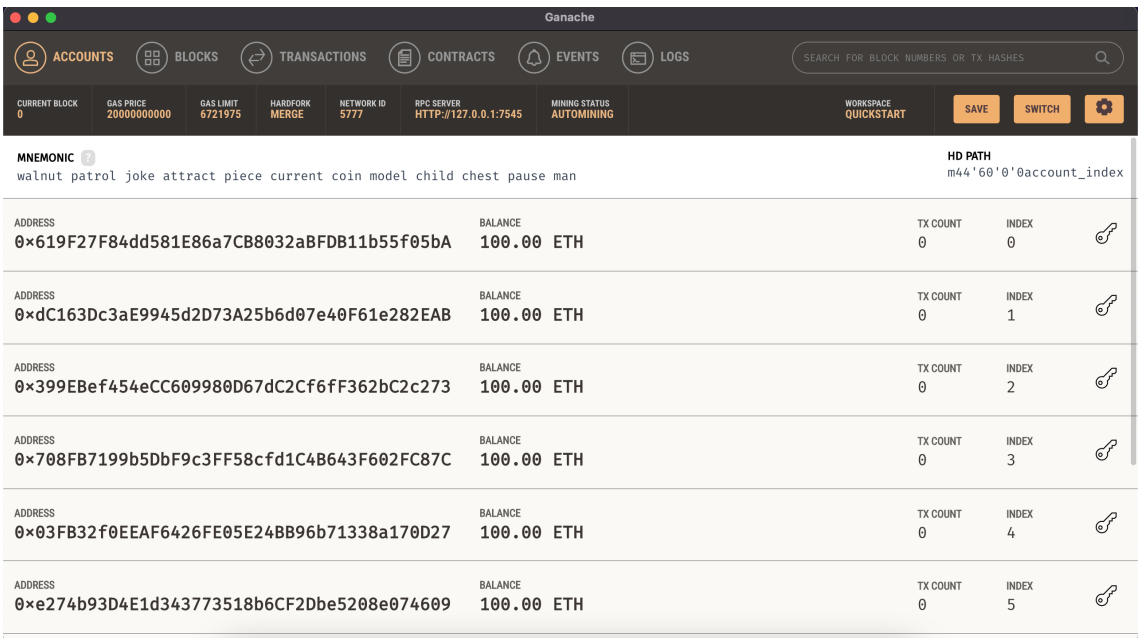


Slika 5.2 Faza autentifikacije - dijagram toka

5.2.3 Konačno rješenje

U nastavku je prikazan primjer korištenja programskog rješenja biometrijske autentifikacije.

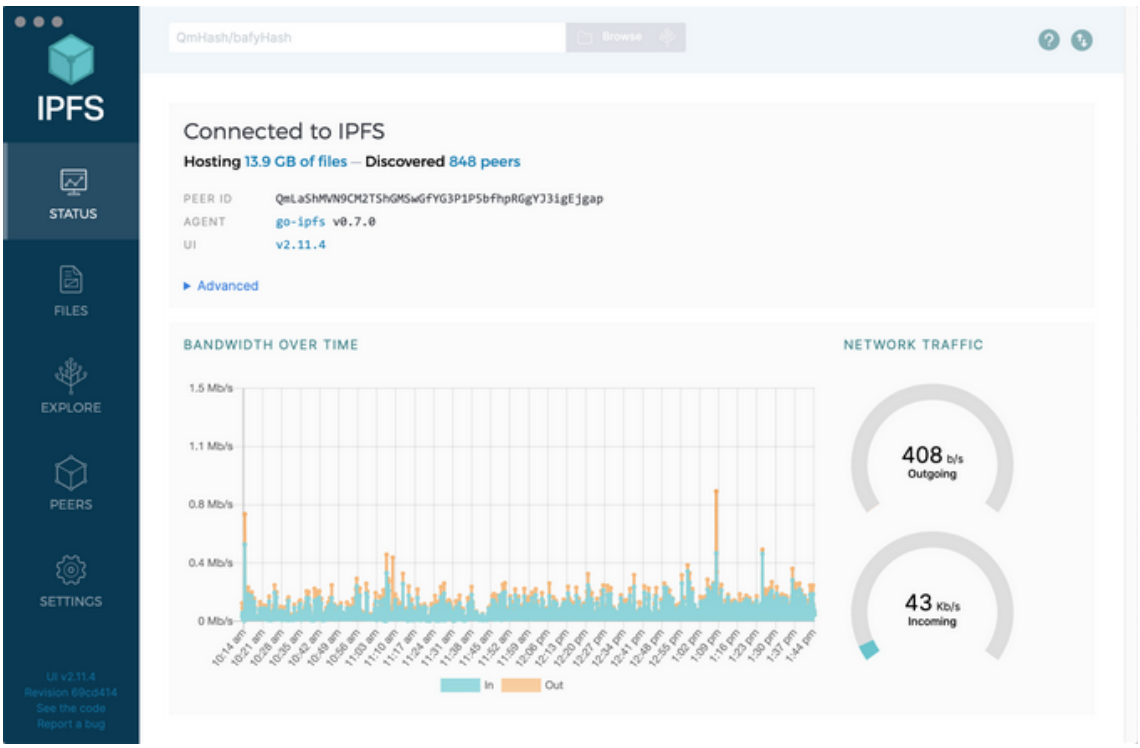
Kao prvi korak potrebno je pokrenuti Ganache aplikaciju te unutar nje odabrati opciju "Quickstart Ethereum" čime stvaramo našu razvojnu blockchain mrežu te nakon toga dolazimo do radnog prostora (slika 5.3) s inicijaliziranom mrežom te računima korisnika koji će obavljati transakcije.



Slika 5.3 Radni prostor Ganache aplikacije

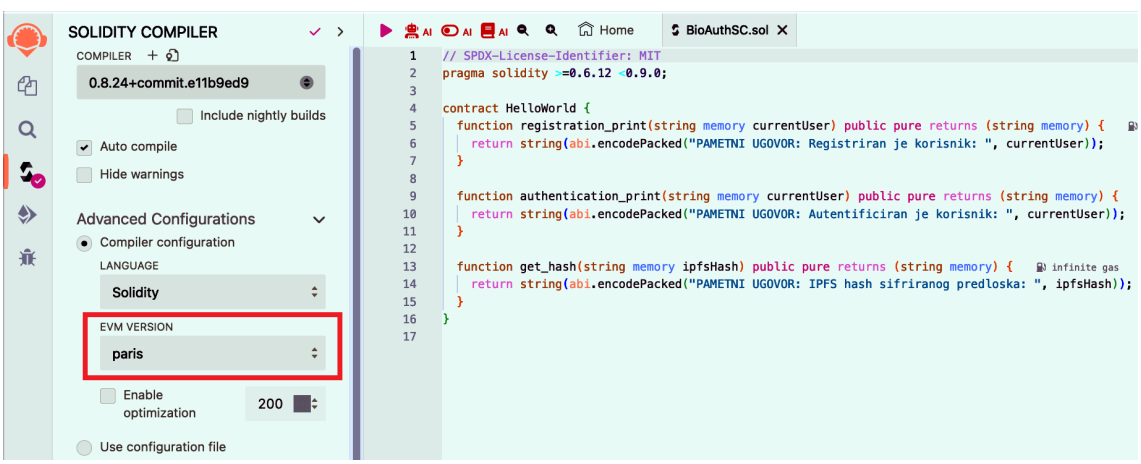
Također, potrebno je pokrenuti IPFS Desktop App (Slika 5.4) kako bi mogli iskoristiti pogodnosti IPFS pohrane.

Završno, prije pokretanja same aplikacije, potrebno je implementirati pametni ugovor na razvojnu Ethereum mrežu. U slučaju ovog diplomskog rada, implementacija se provodi koristeći Remix IDE u kojem je napisan pametni ugovor "BioAuthSC.sol". Prije implementacije pametnog ugovora potrebno je konfigurirati određene parametre izvođenja. Unutar "Advancer Configurations" potrebno je promijeniti op-



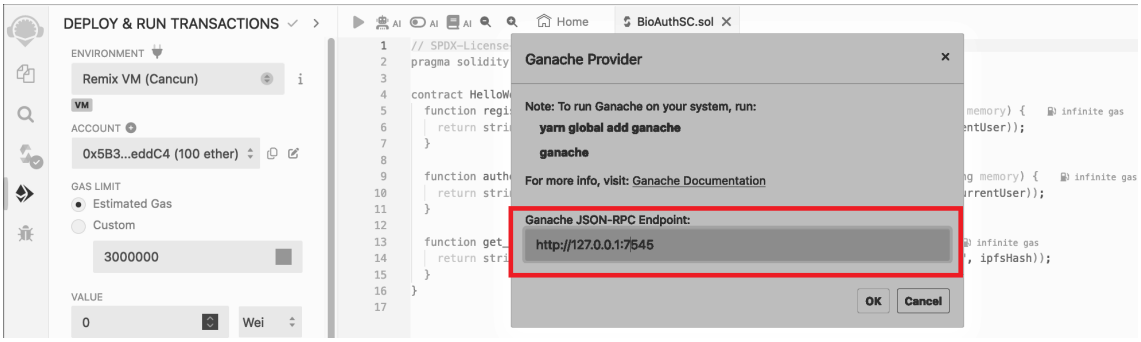
Slika 5.4 Radni prostor IPFS Desktop aplikacije

ciju "EVM version" s "default" na opciju "paris" (Slika 5.5).



Slika 5.5 Remix IDE - prilagodba konfiguracije

Nakon prilagodbe opcije "EVM version" potrebno je povezati Remix IDE s našom Ethereum mrežom. Povezivanje se vrši koristeći opciju "Environment" te odabirom opcije "Dev-Ganache Provider" nakon čega se upisuje adresa Ganache JSON-RPC Endpoint-a (Slika 5.6).

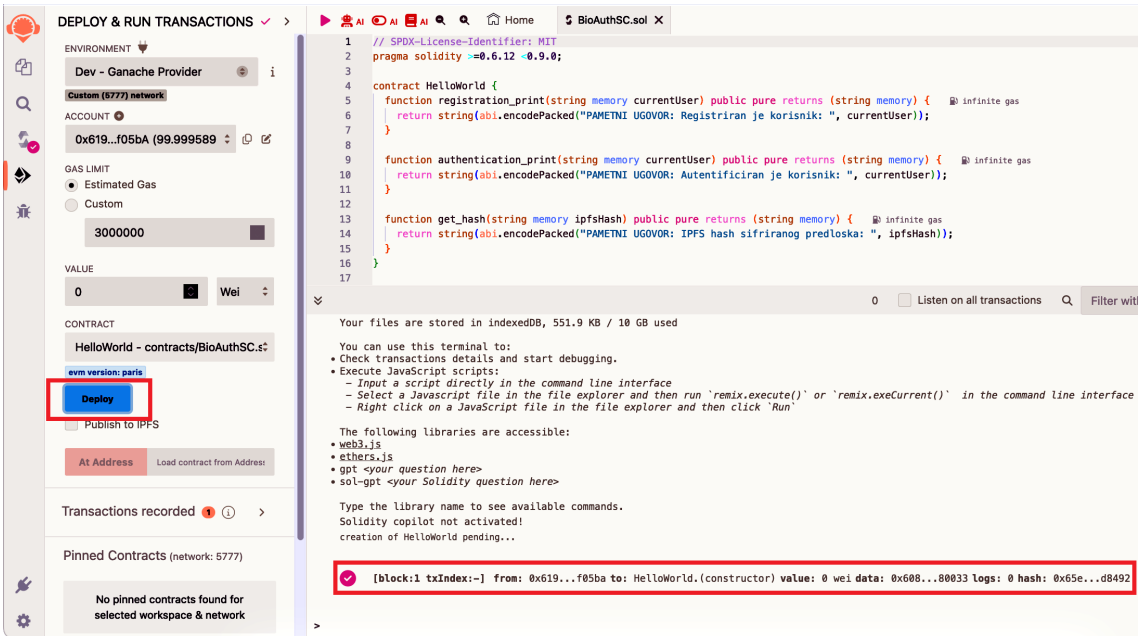


Slika 5.6 Remix IDE - povezivanje na Ganache JSON-RPC Endpoint

Izmjenom potrebnih parametara, spemni smo na izvršiti pametni ugovor na Ethereum blockchainu. Klikom na tipku "Deploy" izvršavamo pametni ugovor te dobivamo potvrdu uspješne implementacije u konzoli Remix IDE-a (Slika 5.7)

Potvrdu uspješne implementacije možemo također vidjeti i u Ganache aplikaciji pod karticom "Transactions" gdje možemo vidjeti da je dodana nova transakcija te adresa implementiranog pametnog ugovora (Slika 5.8). Posljednji korak, postavljanja aplikacije, čini kopiranje adrese pametnog ugovora u Python kod u varijablu "SMART_CONTRACT_ADDRESS".

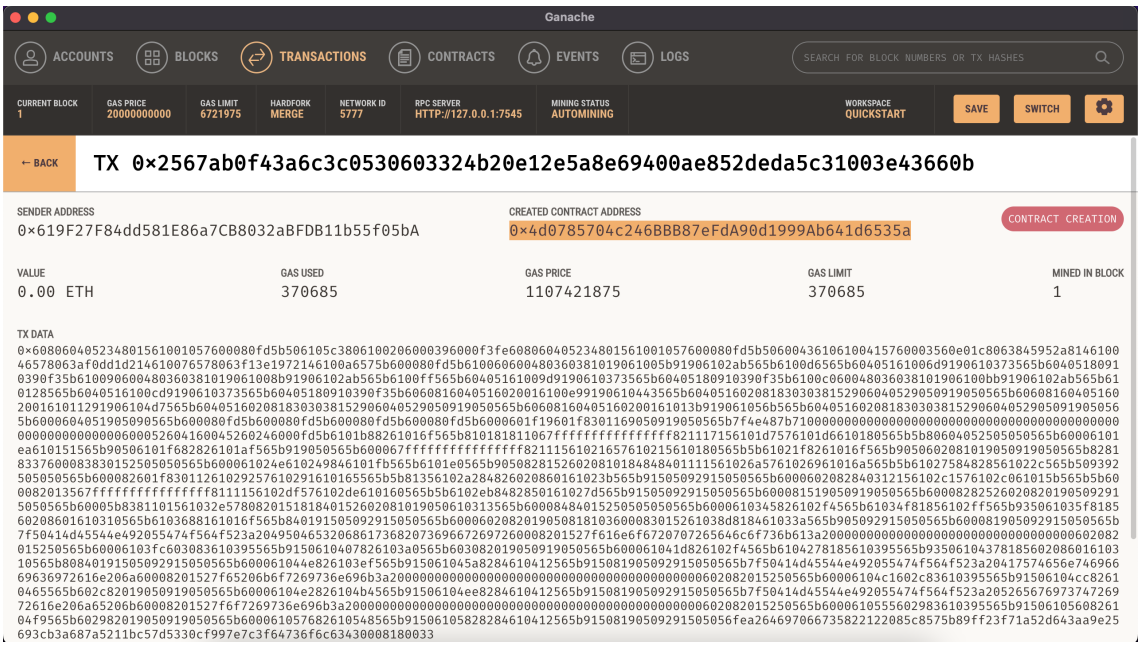
U nastavku, prikazano je izvođenje programskog rješenja biometrijske autentifikacije koriteći blockchain. Slika 5.9 prikazuje kompletan redoslijed izvođenja faze registracije u naredbenom retku. Izvođenje započinje odabirom opcije prikaza vremena izvođenja. Prethodno navedena stavka je potrebna za slijedeće potpoglavlje "Rezultati". Postupak se nastavlja opcijom odabira nastavka kao novi korisnik ili postojeći. Ukoliko se odabere opcija korištenja kao novi korisnik, od korisnika se traži unos imena. Nakon unosa imena, od korisnika se traži izvšenje biometrijskog skeniranja. Pošto u slučaju ovog rada, simuliramo korištenje skenera, korisnik ručno unosi članove biometrijskog predloška. Potom se od korisnika traži unos lozinke. Unosom



Slika 5.7 Remix IDE - implementacija pametnog ugovora

lozinke završava korisnikov angažman u fazi registracije te aplikacija nastavlja svoje izvršavanje kreiranjem privatnog i javnog ključa, njihovom lokalnom pohranom, generiranjem transformacijskog vektora, transformiranjem origirnalnog biometrijskog predloška korištenjem transformacijskog vektora, šifriranjem transformiranog biometrijskog vektora koristeći javni ključ korisnika, pohranom šifriranog predloška na IPFS te dobavkom hash vrijednosti stvorene datoteke, pohranom transformacijskog vektora te konačnim ispisivanjem potvrde registracije koristeći pametni ugovor.

Završetkom faze registracije, počinje izvođenje faze autentifikacije korisnika. Faza autentifikacije započinje ponovnim unosom lozinke kao dodatnom mjerom sigurnosti prilikom procesa autentifikacije. Potom se izvodi simulirano skeniranje novog biometrijskog predloška. U svrhe demonstracije, odlučeno je pružiti korisniku četiri predefinirana predloška, za što brže i jednostavnije testiranje, te je pružena mogućnost unosa novog biometrijskog predloška. Nakon izvođenja novog skeniranja, izvodi se transformacija novog biometrijskog predloška koristeći originalni transformacijski vektor, šifriranje transformiranog biometrijskog vektora koristeći korisnikov javni



Slika 5.8 Ganache - potvrda implementacija pametnog ugovora

ključ, računanje euklidske udaljenosti biometrijskog predloška pruženog za vrijeme registracije i onog pruženog u fazi autentifikacije, izračunata udaljenost se potom dešifrira te se na temelju zadane granice donosi odluka je li trenutni korisnik uspješno autentificiran ili ne. Kao završni korak, u slučaju uspješne autentifikacije, se izvodi pametni ugovor koji pruža potvrdu o uspješnoj autentifikaciji (Slika 5.10).

Ukoliko je korisnik već obavio proces registracije, te izradio svoj biometrijski predložak, prilikom procesa registracije odabire opciju da želi koristiti aplikaciju kao postojeći korisnik te mu se izlistava popis registriranih korisnika (Slika 5.11). Potom, pretražuje listu korisnika te upisuje redni broj ispred svog imena. Postupak se nastavlja upisom lozinke korisnika kako bi se utvrdilo je li zbilja ta osoba vlasnik tog računa. Ukoliko je lozinka ispravna, izvršavanje se nastavlja dohvaćanjem svih potrebnih podataka korisnika (javni i privatni ključ, transformacijski vektor te šifrirani biometrijski predložak).

Završno, slika 5.12 prikazuje tok izvođenja neispravne autentifikacije korisnika.

Slika 5.9 Konačno rješenje - postupak registracije novog korisnika

Slika 5.10 Konačno rješenje - izvođenje uspješne autentifikacije

5.2.4 Rezultati

U sklopu rada, provedeno je testiranje rješenja na prosječnom računalu opremljenom s dvojezgrenim procesorom Intel Core i5 2.7GHz te 8 GB radne DDR3 memorije.

Pošto se radi o simulaciji korištenja biometrijskih vektora, duljina biometrijskih vektora je postavljena na 5 kako bi se što brže i jednostavnije unio biometrijski vektor

Slika 5.11 Konačno rješenje - postupak registracije postojećeg korisnika

te olakšalo praćenje izvršavanja programa.

Prilikom testiranja, izvršeno je mjerenje vremena određenih segmenata izvršavanja za pojedine faze sustava nalik prikazanom u znanstvenom članku kojeg repliciramo. Vrijeme izvršavanja programa je bilježeno tijekom 50 ponavljanja izvođenja, a u nastavku su prikazane prosječne vrijednosti zabilježenih mjerenja.

Kako bi procijenili performanse sustava, izvršeno je mjerenje vremena niza eksperimenata pri kojima je mijenjana razina sigurnosti pružena BFV algoritmom. Glavni konfiguracijski parametar ključan za sigurnost je polinomni modulus, čija je vrijednost varirala između 1024, 2048, 8192, 16384 te 32768.

Ključne točke u kojima je provedeno mjerenje vremena izvršavanja čine: priprema, transformacija, šifriranje, prijenos, izvršavanje pametnog ugovora te izračun

Slika 5.12 Konačno rješenje - izvođenje neuspješne autentifikacije

udaljenosti. Spomenute točke mjerenja su naznačene na slici 5.13.

Zabilježena opažanja prikazana su tablicom 5.1

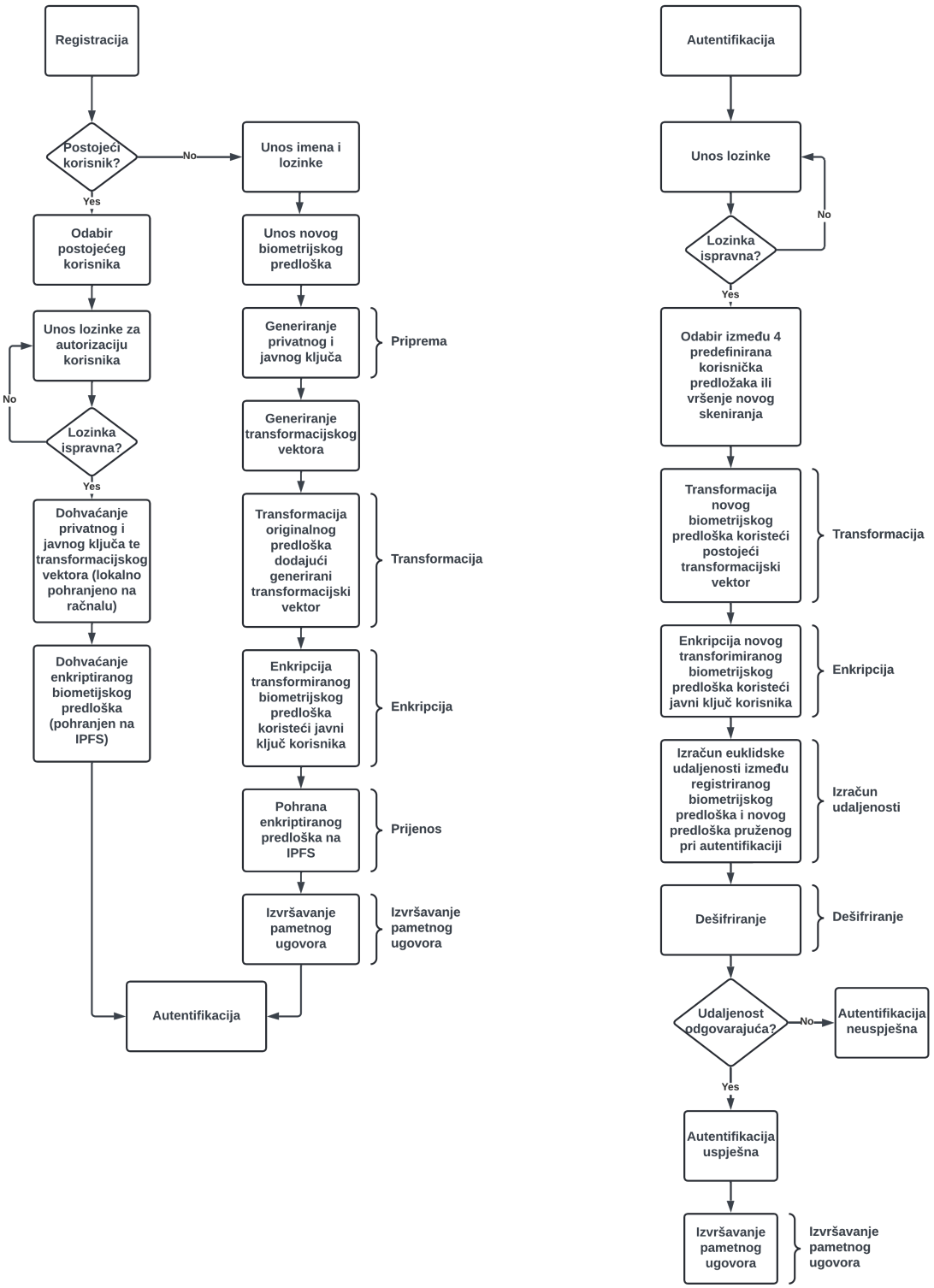
Tablica 5.1 Vremensko trajanje operacija (u sekundama) za različite polinomne module

Operacija	**1024**	**2048**	**4096**	**8192**	**16384**	**32768**
Faza registracije						
Priprema	0.000588	0.001463	0.004443	0.006442	0.023727	0.070862
Transformacija	0.000043	0.000053	0.000047	0.000079	0.000069	0.000073
Šifriranje	0.000583	0.000933	0.003229	0.011532	0.025636	0.077764
Prijenos	Ovisi o IPFS mreži					
Pametni ugovor	Ovisi o Ethereum mreži					
Faza autentifikacije						
Transformacija	0.000054	0.000038	0.000049	0.000089	0.000164	0.000066
Šifriranje	0.000463	0.000806	0.002612	0.008199	0.032689	0.102962
Izračun udaljenosti	0.002489	0.002219	0.005589	0.047315	0.095890	0.399041
Dešifriranje	0.000126	0.000223	0.000799	0.009851	0.017991	0.082055
Pametni ugovor	Ovisi o Ethereum mreži					

Glavni zaključak provođenja niza eksperimenata je da na prosječnom hardveru te s relativno sigurnom opcijom, uzimajući u obzir polinomni faktor, korisnik može registrirati svoj biometrijski predložak u zadovoljavajućem vremenu. U slučaju korištenja polinomnog faktora 4096, registracija biometrijskog predloška traje 0.007719 sekundi.

Preostali koraci registracije ovise o IPFS te Ethereum mreži te nije moguće napraviti univerzalno mjerenje koje bi donijelo zaključak o vremenu izvođenja za ta dva segmenta izvođenja.

Za fazu autentifikacije, provedeno je mjerenje na isti način kao u fazi registracije. Koristeći polinomni faktor 4096, izmjereno vrijeme za fazu autentifikacije iznosi 0.009049.



Slika 5.13 Segmenti u kojima je provedeno mjerenje vremena

Poglavlje 6

Zaključak

U ovom radu detaljno su istražena i uspoređena postojeća rješenja koja implementiraju biometrijsku autentifikaciju na temelju blockchain tehnologije. Analizom rješenja identificirane su prednosti, moguća poboljšanja, performanse te najbolje prakse u primjeni blockhain tehnologija u svrhe biometrijske autentifikacije.

Prateći postupke, ponajviše prikazane člankom [14], napravljena je vlastita implementacija biometrijske autentifikacije koristeći blockchain. Izrađeno rješenje predstavlja konceptualnu ideju koja bi se mogla koristiti u svrhu biometrijske autentifikacije korisnika. Provedeno je testiranje predloženog rješenja koristeći Ganache razvojnu Ethereum mrežu te je provedeno dokumentiranje rezultata. Promatranja vremena izvršavanja pojedinih segmenata programa pružaju uvid u performanse predložene implementacije, naglašavajući potencijal za daljnje optimizacije i poboljšanja.

Blockchain tehnologija sa svojim svojstvima poput distribuiranosti, otvorenosti, neizmjenjivosti te samoodrživosti, otvara vrata za daljnji razvoj aplikacija u raznim područjima. Imajući na umu navedeno, blockchain se pojavljuje kao jedan od ključnih elemenata sigurnosnih sustava budućnosti pa tako i u pogledu biometrijske autentifikacije. Ključ uspjeha takvih tehnologija je pažljivo razmatrati sigurnosne aspekte kako bi se osiguralo njihovo pouzdano i sigurno funkcioniranje. Pitanja privatnosti postaju sve važnija, osobito kada su u pitanju osjetljivi biometrijski podaci. Biometrijski podaci su izuzetno osjetljivi i zahtijevaju visoku razinu zaštite kako bi se

osiguralo da se koriste isključivo za namjenjene svrhe te kako bi se spriječilo njihovo neovlašteno curenje.

Također, performanse su vrlo važan faktor. Sustavi koji koriste biometrijsku autentifikaciju unutar blockchain okvira moraju pružiti zadovoljavajuće performanse bez dodatnih kašnjenja prilikom korištenja.

U konačnici, ključ uspjeha leži u pažljivom planiranju, implementaciji strogih sigurnosnih protokola i poštivanju pravnih normi. Prateći navedene smjernice moguće je stvoriti pouzdane sigurnosne sustave koji će iskoristiti puni potencijal biometrijske autentifikacije unutar blockchain tehnologije.

Bibliografija

[1] "Youverify", Priscilla: "Identification Vs Verification Vs Authentication", s Interneta, https://youverify.co/blog/identification-verification-authentication, 1. svibnja 2024.

[2] "TechTarget", Alexander S. Gillis, i dr.: "What is biometrics?", s Interneta, https://www.techtarget.com/searchsecurity/definition/biometrics, 15. travnja 2024.

[3] "Aware", "Biometric Processes", s Interneta, https://www.aware.com/what-are-biometrics-biometric-processes/, 16. travnja 2024.

[4] "Stanford Online", "How does blockchain work?", s Interneta, https://online.stanford.edu/how-does-blockchain-work, 15. ožujka 2024.

[5] "Forbes", Bernard Marr: "The 5 Biggest Problems With Blockchain Technology Everyone Must Know About", s Interneta, https://www.forbes.com/sites/bernardmarr/2023/04/14/the-5-biggest-problems-with-blockchain-technology-everyone-must-know-about/, 15. ožujka 2024.

[6] "TechTarget", Amanda Hetler: "Proof of work vs. proof of stake: What's the difference?", s Interneta, https://www.techtarget.com/whatis/feature/Proof-of-work-vs-proof-of-stake-Whats-the-difference, 17. ožujka 2024.

[7] "Nerdwallet", Andy Rosen: "Proof of Work (PoW): Definition and Examples", s Interneta, https://www.nerdwallet.com/article/investing/proof-of-work, 17. ožujka 2024.

[8] "Nerdwallet", Andy Rosen: "Proof of Stake (PoS) in Crypto: Here's What it Means", s Interneta, https://www.nerdwallet.com/article/investing/proof-of-stake, 17. ožujka 2024.

[9] "Investopedia", The Investopedia team: "What Are Smart Contracts on the Blockchain and How Do They Work?", s Interneta, https://www.investopedia.com/terms/s/smart-contracts.asp, 19. ožujka 2024.

[10] "Medium", The Novice Freelancer: "A Beginner's Guide to InterPlanetary File System (IPFS)", s Interneta, `https://medium.com/@TheNimbleNovice/a-beginners-guide-to-interplanetary-file-system-ipfs-d83232dc39a5`, 20. ožujka 2024.

[11] Oscar Delgado-Mohatar, i dr.: "Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends", arXiv:2003.09262v1 [cs.CV] 19 Mar 2020

[12] "Investopedia", The Investopedia team: "Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain", s Interneta, `https://www.investopedia.com/terms/g/gas-ethereum.asp`, 10. svibnja 2024.

[13] Youn Kyu Lee, Jongwook Jeong: "Securing biometric authentication system using blockchain", ScienceDirect Volume 7, Issue 3, September 2021., Pages 322 - 326

[14] F. Toutara, G. Spathoulas, "A distributed biometric authenti-cation scheme based on blockchain," in 2020 IEEE International Conference on Blockchain (Blockchain). IEEE, 2020, pp. 470 - 475

[15] "Github", ipfs-shipyard: "py-ipfs-http-client", s Interneta, `https://github.com/ipfs-shipyard/py-ipfs-http-client`, 5. veljače 2024.

[16] "NumPy", s Interneta, `https://numpy.org/`, 5. veljače 2024.

[17] "Python", "getpass — Portable password input", s Interneta, `https://docs.python.org/3/library/getpass.html`, 5. veljače 2024.

[18] "Python", "json — JSON encoder and decoder", s Interneta, `https://docs.python.org/3/library/json.html#module-json`, 5. veljače 2024.

[19] "Python", "time — Time access and conversions", s Interneta, `https://docs.python.org/3/library/time.html#module-time`, 5. veljače 2024.

[20] "Python", "os — Miscellaneous operating system interfaces", s Interneta, `https://docs.python.org/3/library/os.html#module-os`, 5. veljače 2024.

[21] "Github", pipermerriam: "web3.py", s Interneta, `https://github.com/pipermerriam/web3.py`, 1. veljače 2024.

[22] "Github", Microsoft: "SEAL", s Interneta, `https://github.com/microsoft/SEAL`, 1. veljače 2024.

[23] "Github", Huelse: "Microsoft SEAL For Python", s Interneta, `https://github.com/Huelse/SEAL-Python`, 1. veljače 2024.

[24] "Truffle Suite", "Ganache", s Interneta, `https://archive.trufflesuite.com/ganache/`, 3. veljače 2024.

[25] "Remix IDE", s Interneta, `https://remix.ethereum.org/`, 6. veljače 2024.

[26] "IPFS Desktop App", s Interneta, `https://docs.ipfs.tech/install/ipfs-desktop/`, 5. veljače 2024.

Sažetak

Ovaj rad istražuje sustave biometrijske provjere autentičnosti koji se temelje na blockchainu te upravljaju biometrijskim informacijama na decentralizirani način. U svrhu izrade predloženo je vlastito, konceptualno rješenje temeljeno na znanstvenom članku [14]. Dokumentacija sadrži opis osnovnih pojmova potrebnih za razumijevanje predloženog rješenja te njegove praktične svrhe.

Ključne riječi **— blockchain, IPFS, biometrija, autentifikacija, decentralizacija**

Abstract

This thesis explores biometric authentication systems, based on blockchain technology, which manage biometric information in a decentralized manner. For the purpose of development, a proprietary conceptual solution based on the scientific article [14] is proposed. The documentation includes a description of the fundamental concepts necessary for understanding the proposed solution and its practical purposes.

Keywords **— blockchain, IPFS, biometrics, authentication, decentralization**