Analiza i testiranje programske podrške za upravljanje digitalnim studentskim bedževima na javnom blockchainu

Domitrović, Leo

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET

Diplomski sveučilišni studij računarstva

Diplomski rad

Analiza i testiranje programske podrške za upravljanje digitalnim studentskim bedževima na javnom blockchainu

Rijeka, rujan 2022.

Leo Domitrović

0069082814

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET

Diplomski sveučilišni studij računarstva

Diplomski rad

Analiza i testiranje programske podrške za upravljanje digitalnim studentskim bedževima na javnom blockchainu

Mentor: prof. dr. sc. Kristijan Lenac

Rijeka, rujan 2022.

Leo Domitrović

0069082814

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
POVJERENSTVO ZA DIPLOMSKE ISPITE

Rijeka, 15. ožujka 2022.

Zavod: **Zavod za računarstvo**
Predmet: **Napredni operacijski sustavi**
Polje: **2.09 Računarstvo**

ZADATAK ZA DIPLOMSKI RAD

Pristupnik: **Leo Domitrović (0069082814)**
Studij: Diplomski sveučilišni studij računarstva
Modul: Računalni sustavi

Zadatak: **Analiza i testiranje programske podrške za upravljanje digitalnim studentskim bedževima na javnom blockchainu / Analysis and testing of software for management of digital student badges on public blockchain**

Opis zadatka:

Proučiti, analizirati i usporediti postupke izrade i izdavanja nezamjenjivih tokena (engl. Non-fungible tokens, NFT) na poznatijim javnim blockchain mrežama. Predložiti nekoliko javnih blockchain mreža za implementaciju digitalnih studentskih bedževa u obliku nezamjenjivih tokena.

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

Leo Domitrović
Zadatak uručen pristupniku: 21. ožujka 2022.

Mentor:

Prof. dr. sc. Kristijan Lenac

Predsjednik povjerenstva za diplomski ispit:

Prof. dr. sc. Kristijan Lenac

IZJAVA

Sukladno članku 8. pravilnika o diplomskom radu, diplomskom ispitu i završetku diplomskih sveučilišnih studija Tehničkog fakulteta Sveučilišta u Rijeci od 31. siječnja 2020., izjavljujem da sam samostalno izradio/izradila diplomski rad prema zadatku preuzetom dana 21. ožujka 2022.

Rijeka, 20. rujna 2022.

_____

Leo Domitrović

Sadržaj

1. UVOD

Cilj ovog rada bio je proučiti i testirati postupke izrade nezamjenjivih *tokena* (eng. *Non fungible token* – NFT) na različitim *blockchain* mrežama i predložiti koja je od njih najbolja za korištenje. Nezamjenjivi *token* je *token* koji je jedinstven, tj. ne postoje dva ista nezamjenjiva *tokena*. U današnje vrijeme, sve je popularnije da umjetnici stvaraju digitalne umjetnine, glazbenici pjesme, a fotografi fotografije i prodaju ih na internetu. Tu u priču ulazi NFT koji je dokaz da su baš oni stvorili taj medijski sadržaj. Kod kupnje NFT-ova se plaća se u matičnoj kriptovaluti odabrane *blockchain* mreže.

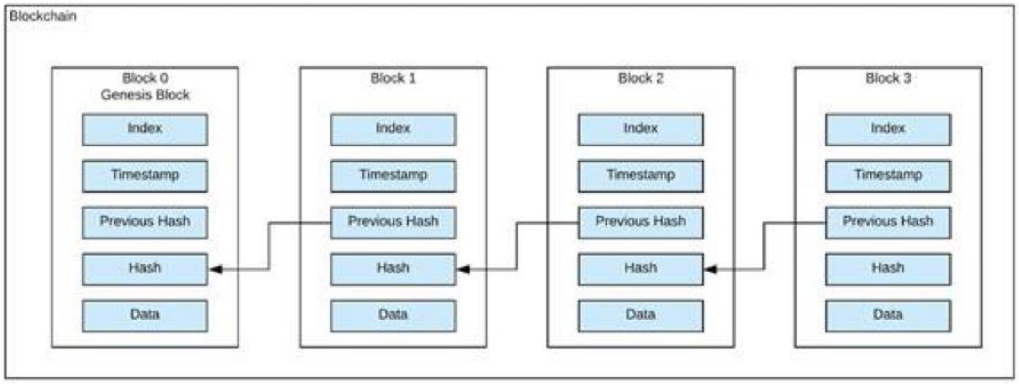
Izrada NFT-ova bit će testirana na Algorand, Ethereum, Near, Cosmos i Cardano blockchain mrežama. Sve navedene *blockchain* mreže već imaju implementirano sučelje za izradu NFT-ova. Ipak, svaka mreža pruža dokumentaciju za izradu kako bi se mogao sa vlastitog računala izraditi NFT na određenom *blockchainu*, kao da je izrađen na službenoj web stranici.

Istraživanje i testiranje u ovom radu dio je projekta digitalnih studentskih bedževa. Početna je ideja projekta omogućiti izdavanje odgovarajućih digitalnih bedževa studentima u sklopu Riteh Blockchain Teama. Vrste bedževa koje trenutno postoje su osnivač tima, voditelj projekta i član projektnog tima, ali i mnoge druge. Pod meta-podacima nalaze se informacije o pojedinog bedžu kojeg osoba dobije. U ovom trenutku bedževi vrijede samo za članove Riteh Blockchain Teama, ali cilj je dodatno proširiti njihovu primjenu na cijeli Tehnički fakultet. Osobe koje posjeduju određeni bedž mogu vrlo lako dokazati da posjeduju specificirane vještine te na račun toga moguće zaraditi i neke povlastice.

U prvom poglavlju opisuju se *blockchain* i *blockchain* tehnologije koje omogućavaju izradu, upravljanje i trgovanje nezamjenjivim *tokenima*. Zatim su detaljnije predstavljeni nezamjenjivi *tokeni* te *blockchain* mreže na kojima će biti testirana izrada nezamjenjivih *tokena*. Na kraju su prikazani rezultati testiranja izrade nezamjenjivih *tokena*.

2. BLOCKCHAIN I PAMETNI UGOVORI

Blockchain je vrsta baze podataka gdje se podaci pohranjuju u javnu memoriju sličnu knjizi. Model *blockchaina* predstavio je 2008. godine programer/a pod pseudonimom Satoshi Nakamoto, a već sljedeće godine su implementirali prvi *blockchain* pod nazivom Bitcoin [1]. U *blockchainu* korisnici stvaraju i postavljaju transakcije na *blockchain*. Svaku transakciju potpisuje stvaratelj da bi bila ispravna jer potpis označava dopuštenje za određenu akciju [2]. Različiti *blockchainovi* imaju različite načine provjere ispravnosti transakcija, a u nastavku rada će biti opisani mehanizmi koje koriste *blockchainovi* korišteni u ovom radu. Ako je provjera uspješna, blok sa određenim brojem transakcija se dodaje u lanac na *blockchainu* te tu ostaje zauvijek [2]. Blok se u budućnosti više neće moći izmijeniti niti obrisati. Svaki blok ima jedinstveni *hash* (znakovni niz koji sadrži slova i brojeve). Blokovi se ulančavaju tako što svaki, osim početnog bloka, sadrži *hash* prethodnog bloka, a o tom *hashu* ovisi i *hash* trenutnog bloka. Izmjena transakcije uzrokuje promjenu *hasha* pa se prema *hashu* provjerava ispravnost transakcije [3]. Ako se uzme u obzir sve rečeno, može se zaključiti da je *blockchain* vrlo siguran i transparentan način pohrane podataka.



Slika 2.1. Blokovi u blockchainu [3]

Važan dio *blockchaina* su čvorovi, a postoje razni čvorovi s različitim funkcijama. Potpuni čvorovi sadrže kopiju cijelog *blockchaina,* tj. svih transakcija te potvrđuju transakcije i blokove. Oni su u svakom trenutku sinkronizirani. Ako se pojavi novi čvor, on se sinkronizira sa jednim od potpunih čvorova. Postojanje potpunih čvorova daje dodatnu sigurnost u slučaju kvara određenog čvora ili nestanka struje jer i dalje postoji kopija od drugih potpunih čvorova. Potpuni čvor može sadržavati kopiju cijelog *blockchaina* ili samo određeni broj blokova, ako nema dovoljno memorijskog prostora za pohranu cijelog *blockchaina.* Lagani čvorovi pohranjuju podatke i pružaju samo obavezne informacije kako bi omogućile brže transakcije i olakšale obavljanje dnevnih zadataka. Oni ne potvrđuju blokove te pohranjuju samo zaglavlje blokova [4]. U slučaju da lagani čvor želi

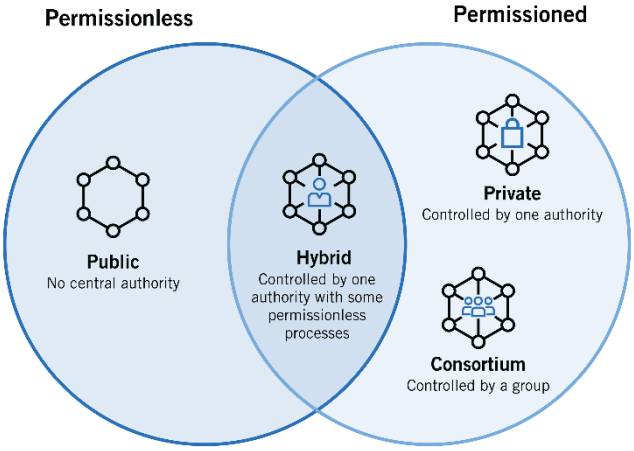
poslati transakciju, mora ju poslati potpunom čvoru koji onda transakciju dodaje u *blockchain*. Kripto novčanici su lagani čvorovi. Rudarski (eng. miner) čvorovi su potpuni čvorovi koji potvrđuju transakcije i dodaju ih u blokove [5]. Glavni čvorovi (eng. Masternode) potvrđuju i pohranjuju transakcije, ali imaju i dodatne bitne funkcije. Ti čvorovi mogu imati pravo glasovanja u slučaju uvođenja određenih promjena u mrežu te osiguravati da se prate pravila i protokoli u *blockchainu* u kojem se nalaze. Kako bi netko bio glavni čvor, mora založiti određenu količinu kripto sredstava. Ako prekrši pravila *blockchaina* na kojem se nalazi, uzimaju mu se založena sredstava. Za iskreno djelovanje glavni čvor dobije godišnju nagradu, određeni postotak založenih sredstava [6].

Najvažnija primjena *blockchaina* je u transakcijama *tokena*. Svaka transakcija se vidi na *blockchainu* i javno je dostupna. U svakom trenutku moguće je preko određenog ključa vidjeti sve transakcije u kojima je jedan korisnik sudjelovao, bilo da je bio primatelj ili pošiljatelj. Ključ po kojem je moguće pretraživati može biti adresa novčanika primatelja ili pošiljatelja, jedinstvena identifikacijska oznaka transakcije i visine bloka. U slučaju pretraživanja po visini vidljive su informacije o bloku i sve transakcije u tom bloku [7].

Kripto novčanici su spremnici osjetljivih korisničkih informacija. U njemu se nalaze privatni ključevi potrebni za slanje transakcija i trošenje sredstava na računu. Privatni ključ se ne smije nikome otkriti. Svaki novčanik ima veliki broj javnih ključeva, a bilo koji od njih može se iskoristiti kao javna adresa novčanika za primanje sredstava [8]. Novčanici sadrže i prikaz svih transakcija u kojima je korisnik sudjelovao, i kao pošiljatelj i kao primatelj [nešto]. Postoje razne vrste kripto novčanika, a to su papirnati, softverski i hardverski. Papirnati novčanik znači da su ključevi i *seed* fraza jednostavno zapisani na papir. *Seed* fraza je fraza koja sadrži određeni broj riječi te se koristi za ponovno pristupanje izgubljenom kripto novčaniku. Softverski novčanik je pohrana ključeva u aplikaciji ili nekom drugom programu. Najsigurniji su hardverski novčanici, gdje su ključevi sigurno pohranjeni na uređaj koji se priključi na računalo samo kada je potrebno te u niti jednom trenutku nisu dostupni na računalu [9].

2.1. Vrste blockchainova prema načinu upravljanja i pristupu

Blockchainovi mogu biti javni, privatni, hibridni i konzorcijski. Javnim *blockchainom* nitko ne upravlja i može se bilo tko priključiti. Svi čvorovi imaju jednaka prava u javnom *blockchainu*. S druge strane, privatni *blockchain* je centraliziran i u njemu mogu sudjelovati samo čvorovi kojima to dopusti organizacija koja upravlja *blockchainom*. Dodatno, nije nužno da svi čvorovi imaju jednaka prava pa određeni čvorovi mogu imati manja prava od ostalih. Konzorcijski *blockchain* je sličan privatnom, samo što u ovom slučaju konzorcij ili grupa organizacija upravlja mrežom. Problem ove vrste je potreba za suradnjom između organizacija koje upravljaju hibridnim *blockchainom* te potreba za sporazumom oko svih odluka. Hibridnim *blockchainom* upravlja jedna organizacija, kao kod privatnog, uz korištenje javnog *blockchaina*. Veće organizacije koriste hibridni *blockchain* kako bi poboljšali efikasnost rada. Privatni i javni *blockchainovi* ima svoje prednosti i nedostatke. Javni *blockchain* je zbog većeg broja čvorova i decentralizacije sigurniji od privatnog jer ima više čvorova koji mogu potvrditi transakcije, ali veći broj čvorova dovodi do duže obrade svake transakcije. Kod privatnog je obrada brža, ali i veća je vjerojatnost pojave loših čvorova pa je vrlo važno da se u *blockchain* ne uključuju sumnjivi čvorovi [12].

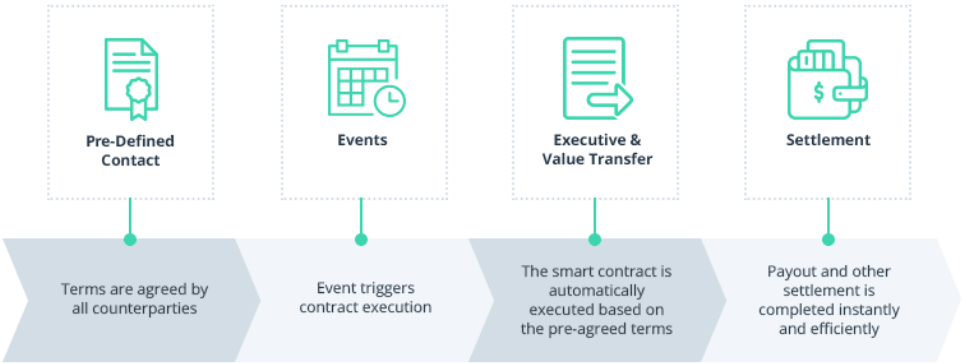


Slika 1.1.1. Vrste blockchainova [12]

2.2. Pametni ugovor

Pametni ugovor je program pohranjen na *blockchainu* koji se automatski i odmah izvršava kad se ispune predefinirani uvjeti [19]. Znanstvenik Nick Szabo definirao ih je 1994. godine računalne transakcijske protokole koji izvršavaju uvjete ugovora. Kada je programski kod ugovora ispravan,

ne može se dogoditi da se program izvrši kada nisu bili ispunjeni svi uvjeti. On predstavlja (digitalni) ugovor u kojem su stvarni uvjeti dogovora između kupca i prodavača zapisani u obliku programskog koda [20]. Prva *blockchain* mreža na kojoj su se pametni ugovori pojavili je Ethereuem te je nakon toga njihova primjena samo rasla [21]. Kada pametni ugovor dobije sredstva od korisnika, svi čvorovi izvršavaju pametni ugovor kako bi se provjerilo dobivaju li isti rezultat nakon izvršavanja. Na taj način nepoznati korisnici s bilo kojih mjesta u svijetu mogu međusobno vršiti pouzdane transakcije bez potrebe za centralnim tijelom, npr. bankom, koje bi provjeravalo transakciju [22]. Time se osigurava da se transakcija izvrši bez kašnjenja koje bi se pojavilo čekanjem da centralno tijelo obradi transakciju, ali i naknadama koje bi sudionici plaćali posrednicima da provjere transakciju [19]. Kod pametnih ugovora se plaća naknada za postavljanje pametnog ugovora u određeni lanac na *blockchainu* te za njegovo izvršavanje [23]. Kod definiranja uvjeta ugovora važno je pokriti sve moguće iznimke koje se mogu dogoditi, a potrebno je definirati i načine rješavanja nesuglasica [19].



Slika 2.2.1. Tijek događaja kod pametnog ugovora

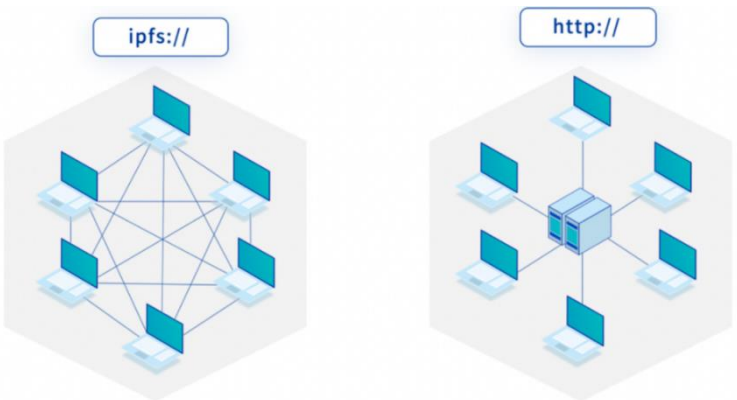
Pošto je šifrirani pametni ugovor pohranjen na *blockchainu* i nema posrednika, teško ga sudionici ili napadači mogu naknadno izmijeniti u svoju korist [15]. Također, ugovor se ne može niti poništiti [22]. Kako se pametni ugovori nalaze u digitalnom obliku na *blockchainu*, nema potrebe za razmjenom ugovora u papirnatom obliku jer ih svaki sudionik u svakom trenutku može vidjeti na *blockchainu*. Prednost pohrane pametnog ugovora na *blockchainu* je i u tome što svaki potpuni čvor na *blockchainu* ima ugovor te će zbog toga biti uvijek dostupan za pregled i izvršavanje [22]. Međutim, pohrana na *blockchainu* predstavlja i nedostatak jer se ne može izmijeniti ako se naknadno pojavi novi uvjet. U tom slučaju potrebno je izraditi novi pametni ugovor sa dodatnim uvjetom koji se pojavio [24].

Primjer pametnog ugovora može biti i potpora određenog *startup* projekta te tada korisnici mogu uložiti određenu količinu novca u taj projekt. Pametni ugovor se aktivira kad se postigne određeni cilj, npr. u projekt je uložena željena količina novca, i tek tada vlasnik projekta prima sredstva koja su uložena u projekt. U suprotnom se korisnicima koji su ulagali u projekt vraćaju uložena sredstva [25].

Razvoj pametnih ugovora je moguć na velikom broju *blockchainova*, a najpoznatiji je Ethereum [26]. Za razvoj se može iskoristiti jedan od postojećih alata za razvoj pametnog ugovora na željenom *blockchainu*. Pametni ugovori se mogu pisati u raznim programskim jezicima, a najpopularniji su Solidity, Rust i JavaScript [27].

2.3. IPFS (InterPlanetary File System)

IPFS (eng. *InterPlanetary File System*) je decentraliziran distribuiran sustav za pristup i pohranu datoteka, podataka, web stranica i aplikacija [28]. Jedna od primjena IPFS-a je pohrana slika i meta-podataka nezamjenjivih *tokena*, na taj način su, uz NFT-ove koji se nalaze na *blockchainu*, i njihove slike i meta-podaci decentralizirano pohranjeni. To je *peer-to-peer* mreža [29] u kojoj sudionici u mreži mogu služiti za pohranu informaciju, mogu slati nove podatke u mrežu ili oboje [30]. Sadržaj koji se šalje se dijeli na više dijelova, a dijelovi mogu biti pohranjeni na različitim mjestima u mreži. Svaki čvor za pohranu sadrži kopiju podataka koje želi spremiti, ali iz svoje memorije može obrisati sadržaj kojem nitko nije pristupao određeni vremenski period [29]. Razlika između pohrane u IPFS mreži (lijevo) i na centralnom serveru (desno) prikazana je na slici ispod:



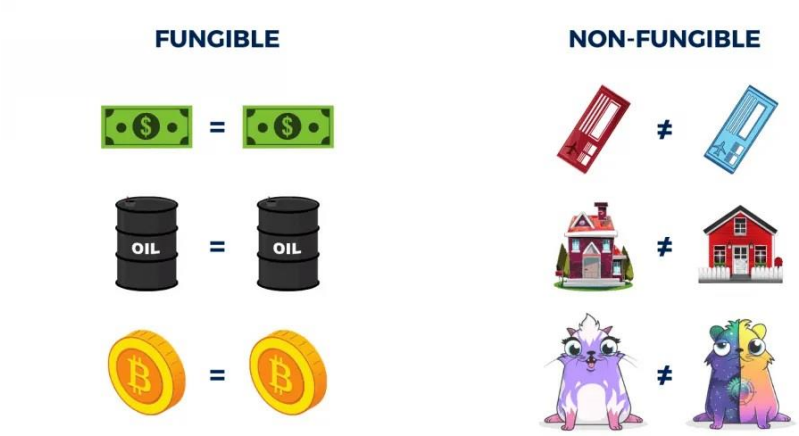
Slika 2.3.1. Razlika između pohrane u IPFS mreži i na centralnom serveru[31]

Zbog decentraliziranosti se ne može dogoditi da web stranica u nekom trenutku nije dostupna. Ako jedan čvor nije dostupan, dijelu web stranici će se pristupiti sa nekog drugog čvora. Svim podacima se pristupa pomoću *hasha* stvorenog prema sadržaju koji se pohranjuje. Time se osigurava da je *hash* jedinstven, tj. ne postoji više podataka sa istim *hashom*. Ako izmijenimo datoteku koja se već nalazi u mreži, prethodna verzija se neće prepisati zato jer će nova datoteka posjedovati drugi *hash*. Tada će se nova verzija dodati u mrežu kao zasebna datoteka što omogućava praćenje verzija podataka. Pošto se sadržaj pohranjuje u dijelovima, postoji mogućnost da će prethodna i nova verzija posjeduju iste dijelove. U tom slučaju će se iskoristiti dio prethodne verzije kako se ne bi zauzimao nepotreban memorijski prostor za nešto što već postoji u mreži [29]. Pristupanje datotekama ili otvaranje web stranica bit će brže jer se više ne nalaze na jednom serveru koji može biti na velikoj udaljenosti od korisnika, već pristup daje čvor koji je bliži korisniku. Dodatno, postojanje velikog broja mogućih izvora pomoću kojih možemo pristupiti podacima otežava blokiranje pristupa sadržaju [28].

Ako korisnik želi samo pristupiti IPFS mreži, a ne želi imati čvor jer neće ništa slati u mrežu i ne želi na računalu pohranjivati sve podatke u mreži, to može napraviti tako da na računalo instalira IPFS *Gateway*. Tek tada može pomoću preglednika pristupiti IPFS mreži kao da se te datoteke ili web stranice nalaze u klasičnoj mreži na serveru. Postoje i razni javni *gateway-i* kojima se pristupa IPFS mreži [32].

3. NEZAMJENJIVI TOKENI (NFT)

Postoje zamjenjivi i nezamjenjivi *tokeni* (NFT). Zamjenjivi *tokeni* se mogu opisati na primjeru kripto-valuta gdje 1 Bitcoin jednog korisnika ima istu vrijednosti kao i 1 Bitcoin koji posjeduje drugi korisnik. Nezamjenjivi *tokeni* predstavljaju digitalnu ili stvarnu imovinu i time dokazuju da je određeni korisnik vlasnik te imovine. Primjeri nezamjenjivih *tokena*: umjetnine, slike, audio i video zapisi. Transakcije NFT-ova su vidljive na *blockchainu* i zbog toga nitko ne može kopirati nešto što već postoji jer je javno dostupan dokaz o tome [10].

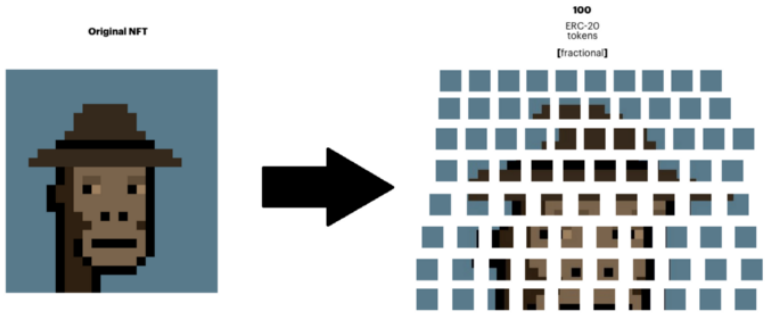


Slika 3.1. Razlika između zamjenjivih i nezamjenjivih tokena [11]

Nezamjenjivi *token* (eng. *Non-fungible token* (NFT)) je jedinstveni element sa jedinstvenim meta-podacima. Nezamjenjivo znači da se ne može zamijeniti s nekom drugom stvari [13], npr. umjetnina se ne može zamijeniti s nekom drugom jer je svaka od njih jedinstvena i ima jedinstvena svojstva. U jednom trenutku može imati samo jednog vlasnika. Svaki NFT imaju svoju identifikacijsku oznaku i nemoguće je da dva nezamjenjiva *tokena* imaju istu oznaku. Ne smiju postojati dvije identične umjetnine ili audio zapisa, pa zato kažemo da su to nezamjenjivi *tokeni* [14]. Mogu se stvoriti i replike jednog originalnog NFT-a gdje su sve replike vrlo slične, ali sve replike i originalni NFT se malo razlikuju. Na taj način su sve replike jedinstvene, a i original ostaje jedinstven [15]. Primjer toga su ulaznice za koncert gdje svaka izgleda gotovo isto, a razlikuju se samo u poziciji na kojoj će se vlasnik NFT-a ili ulaznice nalaziti [14]. Kreirani NFT-ovi se nalaze na *blockchainu* gdje se, ako je na Ethereum *blockchainu*, u svakom trenutku može vidjeti tko je njegov vlasnik, tj. adresa novčanika vlasnika, koliko je vremena proteklo od izrade, povijest prodaja i vlasnika, cijena po kojoj ga možemo kupiti, korišteni pametni ugovor i slično [7]. Postoje različiti NFT standardi, ovisno o *blockchainu* na kojem se izrađuje, a malo će detaljnije

biti opisani standardi koji se koriste na *blockchainovima* korištenim u ovom radu. Dodatno, ovisno o *blockchainu* na kojem će se izraditi NFT, razlikuju se i naknade koje je potrebno platiti. Kod opisa svakog korištenog *blockchaina* prikazan je i način izračuna naknade na pojedinom *blockchainu*. Tvorac NFT-a nakon njegove prvotne prodaje ima mogućnost primanja određenog postotka od svake prodaje tog NFT-a u budućnosti, iako on više nije vlasnik. Postotak se može postaviti u pametnom ugovoru prilikom izrade NFT-a [16]. Svi NFT-ovi kojima je određeni korisnik vlasnik vidljivi su u njegovom novčaniku.

Moguće je izraditi i razlomljeni NFT gdje se jedan jedinstveni nezamjenjivi *token* razlomi na dijelove. Korisnik u slučaju kupnje jednog dijela može reći da je vlasnik dijela nečeg jedinstvenog. Primjer nečega što se može podijeliti na jednake dijelove je nekretnina, pa je vlasnik dijela razlomljenog NFT-a ujedno i vlasnik dijela nekretnine koju NFT predstavlja [17]. Tako korisnici mogu postati suvlasnici željenog NFT-a po manjoj cijeni od one koja bi bila da NFT ima samo jednog vlasnika.



Slika 3.2. Primjer razlomljenog NFT-a [18]

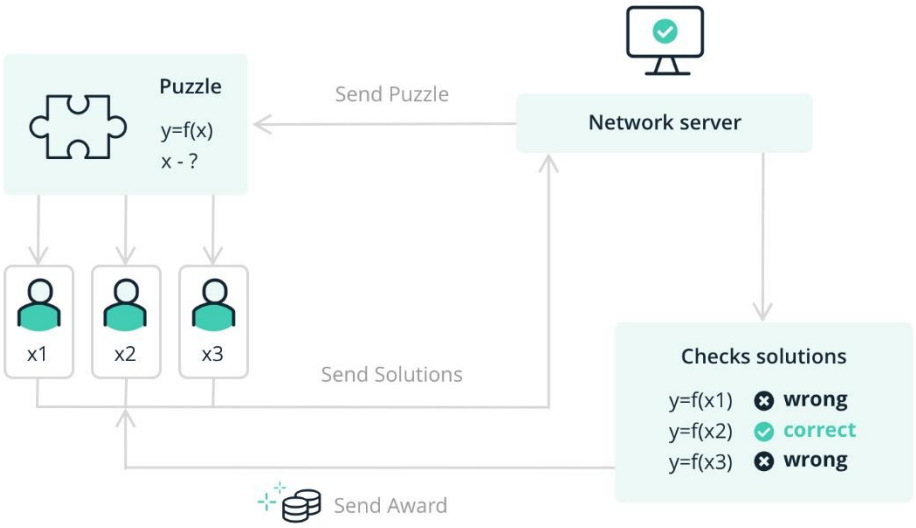
4. ODABRANE BLOCKCHAIN MREŽE

Za izradu nezamjenjivih *tokena* odabrane su Ethereum, Algorand, Cardano, Near i Cosmos *blockchain* mreže. Odabrane su zbog svoje popularnosti te ukupne vrijednosti matičnih *tokena* koji trenutno cirkuliraju mrežom. Također, razlozi odabira su i to što su u aktivnom razvoju i podržavaju pametne ugovore.

4.1. Ethereum

Ethereum je drugi najpopularniji *blockchain* nakon Bitcoin *blockchaina*. Dok Bitcoin *blockchain* služi samo za prijenos kripto-valute Bitcoin između računa, Ethereum je prvi uveo programabilnost, mogućnost razvoja decentraliziranih aplikacija i pametnih ugovora na *blockchainu* [33]. Prosječno se obradi samo 15 transakcija po sekundi [34], što je vrlo malo. Kripto-valuta unutar tog *blockchaina* je Ether [33]. Postoje i privatni *blockchainovi* bazirani na Ethereum *blockchainu* kojeg mogu koristiti veće tvrtke [35]. Za ostvarivanje konsenzusa koristi mehanizam *Proof-of-work* [33].

Proof-of-work je vrlo resursno zahtjevan mehanizam jer zahtjeva od rudarskih čvorova da računaju matematičku funkciju nad skupom podataka kako bi dobili mix*Hash* koji odgovara zadanom cilju *nonce* broja. Cilj *hasha* određuje težinu određivanja, a što je manji cilj, to je manji broj važećih *hasheva*. Što je manji broj mogućih *hasheva*, to će rudarskim čvorovima biti teže pronaći pravi *hash*. Kod potvrđivanja blokova veliki broj rudarskih čvorova se utrkuje kako bi jedan od njih prvi dobio važeći *hash* i uzeo nagradu. Osim što je taj mehanizam zahtjevan za jednog rudarskog čvora koji mora imati poseban hardver da bi odgovorio zahtjevima, potrošnja energije je značajno veća zato jer se veliki broj rudarskih čvorova utrkuje [36]. Zbog postojanja velikog broja rudarskih čvorova koji se u tom trenutku utrkuju da potvrde blok, Ethereum vrlo štetno utječe na okoliš. Na slici ispod nalazi se primjer *proof-of-work* mehanizma u kojem se tri rudarska čvora utrkuju kako bi dobili nagradu. Čvor *x2* je prvi riješio problem te se tada prekinulo izvršavanje i *x2* je dobio nagradu [37].



Slika 4.1.1. Primjer proof-of-work mehanizma [37]

Ethereum je prvi *blockchain* koji je uveo koncept decentraliziranih aplikacija (skraćeno dApp) koji se koristi i na budućim *blockchainovima.* Decentralizirane aplikacije iskorištavaju sve značajke Ethereum *blockchaina*. Pošto se nalazi na *blockchainu* i svi čvorovi imaju kopiju aplikacije, aplikacija će uvijek biti dostupna i vrlo teško ju je blokirati. Za pohranu podataka aplikacija koristi *blockchain*, a logika se nalazi u pametnim ugovorima [38].

Naknade transakcija se računaju na sljedeći način. Uzimaju se u obzir potrebni računalni resursi, osnovna naknada i napojnica koju korisnik odluči dati rudarskom čvoru. Napojnica je iznos koji korisnik odluči izdvojiti kako bi transakcija dobila veći prioritet. Naknada se zatim računa prema sljedećoj formuli:

$$Naknada = Najveći\ broj\ resursa * (osnovna\ naknada\ +\ napojnica) \quad (1)$$

Korisniku se, osim količine Ethera koju prenosi nekom korisniku, s računa skida i naknada. Osnovna naknada se uništava, dok napojnicu dobiva rudarski čvor koji je potvrdio transakciju [39].

Za reprezentaciju NFT-ova na Ethereum *blockchainu* postoji standard ERC-721. Svaki NFT definiran ovim standardom ima svoj identifikator i adresu pametnog ugovora. Više NFT-ova može biti iz istog pametnog ugovora, ali svaki NFT mora imati jedinstveni par identifikator, adresa pametnog ugovora. ERC-721 standard pruža mogućnost prijenosa NFT-a na drugi račun te dobivanja informacija o trenutnom vlasniku NFT-a i zalihi NFT-a, ali i razne druge mogućnosti

[40]. Dodatno, uz NFT se mogu dodati i njegovi meta-podaci. Neki od parametara meta-podataka su naziv, opis, poveznica do slike NFT-a, npr. u IPFS mreži, i slično [41].

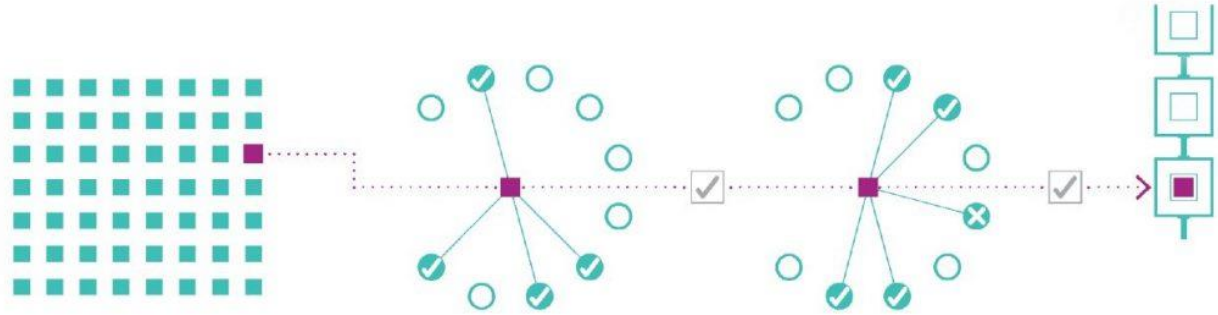
Kako bi se značajno smanjio utjecaj na okoliš, Ethereum *blockchain* je pri završetku pisanja ovog rada prešao na *Proof-of-stake* mehanizam za ostvarivanje konsenzusa. Funkcionira tako da rudarski čvor provjerava jesu li blokovi važeći, a uz svoj glas zalaže i sva kripto valutna sredstva koja ima na računu. Ako se pokaže da je potvrdio blok koji nije ispravan, rudarski čvor gubi založena sredstva, tj. sva sredstva s računa [42].

4.2. Algorand

Algorand je *blockchain* s fokusom na utjecaj na okoliš. Koriste se tehnologije čiji je energetski utjecaj na okoliš puno manji u odnosu na Ethereum [44], što se može vidjeti već po mehanizmu dodavanja blokova u lanac. Za plaćanje naknada unutar Algorand *blockchaina* stvoren je vlastiti *token Algo*. Svatko tko ima određenu količinu Algo-a može se uključiti u proces ostvarivanja konsenzusa. Jezgreni protokol Algoranda je otvorenog koda, a to znači da je javno dostupan i svatko se može uključiti u razvoj. Transakcije su vrlo brzo gotove. Algorand može obraditi 1000 transakcija po sekundi, a te transakcije su nakon obrade i završene. Blokovi se dodaju svakih 4.5 sekunde i mogu sadržavati najviše 5000 transakcija [45]. Ako se najveći broj transakcija po sekundi usporedi sa sadašnjom efikasnosti Ethereum *blockchaina*, može se zaključiti da je Algorand *blockchain* značajno efikasniji, čak oko 66 puta više transakcija po sekundi može obraditi.

Mehanizam dodavanja blokova se zove *Pure Proof-of-Stake* [46]. U procesu može sudjelovati svaki korisnik koji ima određenu količinu sredstava na računu. Ukoliko želi sudjelovati u procesu, mora generirati vlastiti ključ za sudjelovanje kojeg potom koristi u procesu. Odabir korisnika se vrši nasumično i u tajnosti te nitko osim odabranog korisnika ne zna da je on odabran sve dok već nije dao sudjelovao u procesu [47]. U svakoj iteraciji korisnici predlažu blokove koje bi dodali u lanac. Nakon što korisnici predlože blokove odabire se skupina korisnika koji će glasanjem odabrati jedan blok iz svih predloženih. U sljedećem koraku odabire se druga skupina korisnika koja potvrđuje blok koji je prethodna skupina izdvojila. Na kraju svaki čvor dobije certifikat i onda se blok dodaje u lanac na *blockchainu* [46]. Korisnici sa više sredstava na računu će biti češće

odabrani u procesu ostvarivanja konsenzusa [45]. Na slici 4.2.1. nalazi se primjer glasanja korisnika za određeni blok. Na početku je predložen određeni blok. Nakon toga je prikazan primjer glasanja prve skupine korisnika za blok. Zatim je prikazan primjer glasanja druge skupine korisnika za taj blok. Na kraju je prikazano kako je uspješnim glasanjem blok dodan u lanac.



Slika 4.2.1. Primjer ostvarivanja konsenzusa [48]

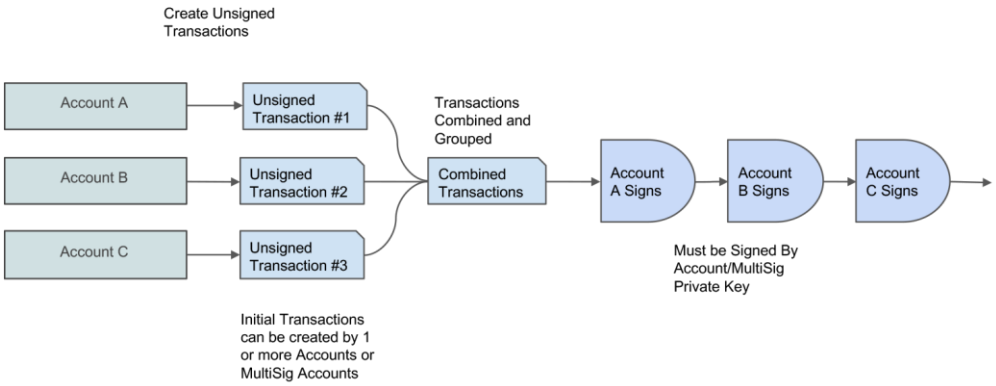
Reprezentacija svake „imovine“ (eng. *asset*), npr. NFT-a u slučaju ovog rada, se odvija vlastitim mehanizmom Algorand *blockchaina*, a to je *Algorand Standard Asset* (ASA) [49]. Njime je omogućeno kreiranje NFT-ova bez potrebe za pisanjem programskog koda za pametni ugovor koji bi identificirao *asset* kao NFT. Na Algorandu se pomoću parametara ASA radi distinkcija između vrsti *tokena* [50]. Izrada je gotova u nekoliko sekundi [49]. Neki od parametara su naziv *asseta*, poveznica na njegove meta-podatke te adrese računa kojima se daje određena kontrola nad *assetom*. Samo parametri sa spomenutim adresama računa se kasnije mogu izmijeniti te se time kontrola može dati nekome drugome. ASA se kasnije može i uništiti, ali samo ako je u vlasništvu računa koji ga je stvorio. Upravitelj *asseta* odlučuje hoće li dopustiti izmjenu parametara i uništavanje. Sa svakim ASA-om koji određeni korisnik stvori ili posjeduje povećava se minimalna količina sredstava koju korisnik mora imati da bi stvorio novi ASA, a poveća se za 0.1 Algo. Ako se pokuša napraviti transakcija u trenutku kada korisnik nema minimalnu količinu sredstava koju mora imati, transakcija će biti neuspješna. Prije nego određeni korisnik može primiti ASA, mora omogućiti primitak [51].

Prednost Algorand *blockchaina* je niska minimalna naknada za transakcije na *blockchain*, a iznosi samo 0.001 Algo (2.51 HRK u trenutku pisanja rada) [45]. Stvarna naknada ovisi o trenutnoj zakrčenosti mreže, a prati se trenutna naknada po bajtu za transakcije u mreži. Računa se prema sljedećoj formuli:

$$Naknada = \max(trenutna\ naknada\ po\ bajtu\ u\ mreži * duljina\ transakcije\ pretvorene\ u\ bajtove, minimalna\ naknada) \quad (2)$$

Ako mreža nije zakrčena, naknada će biti minimalna jer je tada u mreži trenutna naknada po bajtu jednaka 0. U suprotnom, u mreži će trenutna naknada po bajtu biti različita od 0, pa će i naknada za transakciju biti veća od minimalne. U tom trenutku će naknada biti umnožak duljine transakcije pretvorene u bajtove i trenutne naknade po bajtu u mreži [52]. Na taj način se u trenucima zakrčenosti mreže veća važnost daje većim transakcijama, a manje transakcije će biti obrađene kasnije.

Za povezane transakcije na Algorand *blockchainu* postoji *Atomic transfers* mehanizam. On omogućava korisnicima da sigurno razmjenjuju sredstva sa nepoznatim osobama bez potrebe da posrednik provjerava transakcije. Funkcionira tako da se više povezanih nepotpisanih transakcija grupira u jednu jedinicu koja se onda provjerava. Svaka grupa dobiva jedinstveni identifikator koji se potom pohranjuje kao parametar svih transakcija u grupi. Korisnici koji su poslali transakcije potom svoje moraju potpisati, a to rade koristeći svoj privatni ključ. Nakon provjere će sve transakcije biti uspješne ili niti jedna neće uspjeti, ne može se dogoditi da samo nekoliko transakcija prođe. U grupi ne moraju biti samo transakcije istog tipa, već mogu biti transakcije kojima se prenosi određena količina kripto valute Algo nekom korisniku, može se prenositi ASA. Također, u grupi može biti i transakcija upravljana Algorand pametnim ugovorom [53]. Na slici ispod prikazan je slijed događaja.



Slika 4.2.2. Slijed događaja prilikom grupiranja transakcija [53]

4.3. Cardano

Cardano je *blockchain* otvorenog koda koji koristi vlastiti *Proof-of-Stake* mehanizam ostvarivanja konsenzusa. Fokus je na transparentnosti, održivosti i skalabilnosti. Mehanizam ostvarivanja konsenzusa je Ouroboros protokol. Pošto je pisan u Haskell programskom jeziku, Cardano je vrlo siguran *blockchain*. Haskell omogućuje testiranje u izolaciji, prije prelaska na *Mainnet*, kao i razne druge mogućnosti. Testiranjem određene komponente u izolaciji mogu se pronaći i ispraviti sve greške, a da komponenta pritom ne mora biti na Mainnetu. Kripto-valuta za plaćanje naknada na Cardano *blockchainu* je ADA. Cilj je pružiti otpornu i pravednu infrastrukturu za društvene i financijske aplikacije [54]. Cardano može obraditi najviše 250 transakcija u sekundi [55]. To je, kao i slučaju Algoranda, više nego što Ethereum može pružiti, ali je 4 puta manje od kapaciteta Algoranda.

Naknada transakcije uključuje obradu i dugoročnu pohranu transakcije. Kod izračuna minimalne naknade uzimaju se u obzir sljedeći parametri: ovisnost naknade o veličini transakcije, naknada koja se mora platiti neovisno o veličini transakcije i veličina transakcije pretvorena u bajtove. Parametar ovisnosti naknade o veličini transakcije znači da će za veće transakcije biti potrebno više resursa za obradu i pohranu transakcije u mreži, a samim time će biti veća i naknada. Naknada koju korisnici plaćaju neovisno o veličini transakcije sprječava *Distributed-Denial-of-Service* zato jer će ona takve napade činiti preskupim za izvesti. Minimalna naknada se računa po sljedećoj formuli [56]:

$$\begin{aligned} Naknada = {} & ovisnost\ naknade\ o\ veličini\ transakcije \\ & * veličina\ transakcije\ pretvorena\ u\ bajtove \\ & + naknada\ koju\ korisnik\ sigurno\ plaća \end{aligned} \quad (3)$$

Ouroboros protokol je prvi dokazano siguran mehanizam ostvarivanja konsenzusa [57]. Ouroboros radi tako da blokove prvo dijeli na epohe, a epohe zatim dijeli na vremenske prozore. Svaki prozor dobiva voditelja koji bi trebao dodati blok u lanac [59]. Za svakog voditelja se generira ključ za potvrdu i ključ za potpisivanje. Voditelj se nasumično bira sa vjerojatnosti odabira proporcionalnom količini sredstava u početnom bloku. Prema tome, korisnici koji su imali veću količinu sredstava će imati veću vjerojatnost da budu odabrani za voditelja. Svaki voditelj dobiva dokaz da je izabran za voditelja prozora [60]. Taj dokaz će biti sadržan u bloku kojeg je voditelj

dodao kako bi pokazao da je baš on bio zadužen za dodavanje blokova u određenom vremenskom prozoru. Određeni voditelj može prebaciti svoje pravo na sudjelovanje u protokolu (određena sredstva) na *stake pool*. U tom slučaju njegovu zadaću u njegovo ime odrađuje određeni *stake pool* [61]. Kod odabira voditelja će se na *stake pool* gledati kao na korisnika čija je količina sredstava zbrojena količina sredstava korisnika koji su mu povjerili svoja sredstva s računa [58]. *Stake poolovi* obrađuju transakcije te dodaju blokove u lanac. Dovoljan broj korisnika koji posjeduju određena sredstva na računu mora u svakom trenutku biti dostupan kako bi protokol bio siguran. Zauzvrat *stake poolovi* dobivaju nagradu u obliku naknada transakcija i u ovisnosti o trenutnoj zalihi kripto valute ADA. Jedan korisnik je voditelj *stake poola*, dok ostali samo ulažu u *stake pool* [58].

NFT-ovi se identificiraju pomoću parametra policyID. To je identifikator koji je jedinstven i povezan sa NFT-om. Taj identifikator označava skriptu pravila koja definiraju određene značajke NFT-a. Ne može postojati više skripta pravila sa istim identifikatorom. Za razliku od Ethereuema, na Cardano *blockchainu* za sada ne postoji standard za reprezentaciju NFT-a ili njegovih meta-podataka [62]. NFT *asset* mora imati jedinstven par parametara policyID i naziva *asseta* [63]. Određenu skriptu pravila mogu koristiti samo korisnici koji imaju ključ za tu skriptu pravila [64]. Skripta može biti stvorena tako da ju može koristiti jedan korisnik sa svojim setom ključeva, da može biti korištena samo jedanput, tj. samo jednom može biti stvoren *token* s tom skriptom, a može biti stvorena i sa vremenskim ograničenjem. Vremensko ograničenje može biti da se *token* ili *tokeni* mogu stvarati koristeći određenu skriptu samo prije određenog vremenskog prozora ili unutar ili nakon specificiranog vremenskog prozora. Kada vremensko ograničenje istekne, skripta se više neće moći koristiti [65].

4.4. Near

Near je *blockchain* sa fokusom na korisnike i na energetsku učinkovitost. Korisnički računi nisu predstavljeni u obliku adresa, već se koriste nazivi koji su korisnicima jednostavni za razumjeti. Mehanizam ostvarivanja konsenzusa je, kao i slučaju Algorand i Cardano *blockchaina, proof-of-stake*. Transakcije su gotove u samo 1 sekundi. U mreži postoje dvije vrste sudionika, a to su korisnici i *validatori*. Korisnici koriste usluge Near *blockchaina*, a *validatori* izvršavaju blokove i nadziru ostale *validatore* [66], a za svoje iskreno ponašanje dobivaju nagradu jednaku postotku sredstava koje su založili kao jamstvo da će se ponašati iskreno. Vjerojatnost da će određeni

validator biti odabran da provjeri blok proporcionalna je količini sredstava koje je založio [67]. Sudionici u mreži imaju mogućnost prijenosa *asseta* između Near i Ethereuem *blockchaina* korištenjem protokola Rainbow Bridge [68].

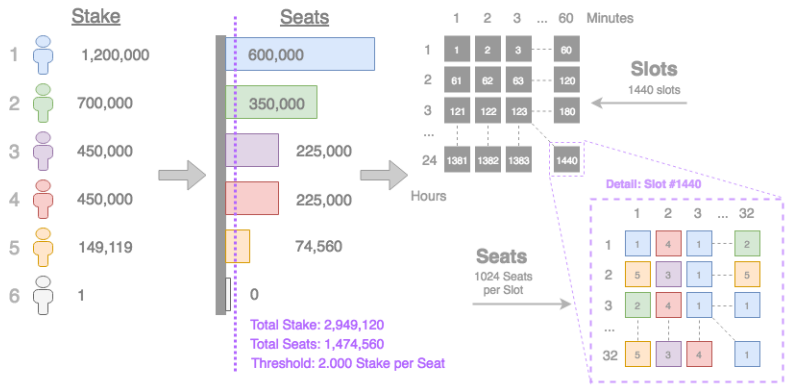
Naknada transakcija sastoji se od tri stavke, a to su: naknada za preuzimanje i prijenos transakcije, naknada za obradu transakcije i naknada za čuvanje transakcije u memoriji. Ukupnu naknadu tako određuju broj procesorskih instrukcija koje je bilo potrebno izvršiti, veličina transakcije u bajtovima i veza između jedinica obrade i prijenosa (što će biti prikazano oznakom α). Formula po kojoj se računa potrebna količina računalnih resursa je prikazana ispod:

$$gas = broj\ procesorskih\ instrukcija\ u\ transakciji + \alpha \\ * veličina\ transakcije\ u\ bajtovima \qquad (4)$$

Nakon izračuna ove varijable potrebno ju je pomnožiti sa trenutnom naknadom za jednu jedinicu računalnih resursa te se tada dobije prvi dio naknade koju je potrebno platiti. Drugi dio naknade predstavlja naknadu koja se plaća čvorovima kako bi držali transakciju u memoriji. Naknada za pohranu u memoriji ovisi o veličini korisničkog računa u bajtova te se njenim množenjem sa cijenom pohrane jednog bajta dobije naknada koju je potrebno platiti [67]. Dodatno, određeni postotak naknada koja se plati za prijenos i obradu transakcije vraća se pametnom ugovoru koji se izvršavao, a na čiji račun će se sredstva prebaciti je specificirano u ugovoru. Početni postotak je 30 %. Sredstva mogu ići programeru koji je razvio korišteni pametni ugovor, investitoru, itd. [69].

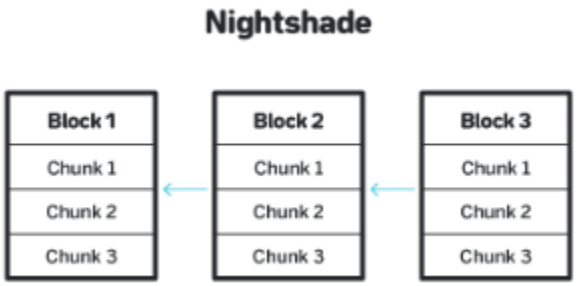
Mehanizam odabira sudionika u procesu ostvarivanja konsenzusa Near *blockchaina* naziva se *Thresholded Proof of Stake*. Odabir sudionika funkcionira kao dražba, tj. korisnici se natječu da budu odabrani za sudjelovanje u procesu ostvarivanja konsenzusa. Svaki korisnik kao prijavu šalje transakciju u kojoj specificira koliko je sredstava spreman založiti za sudjelovanje u procesu u određenom periodu. Korisnici čija je količina založenih sredstava jednaka barem izračunatoj granici bit će odabrani da sudjeluju u procesu onoliko puta proporcionalno količini sredstava koju su založili. Zadan je veliki broj korisnika kako bi se osigurala sigurnost mreže, kako bi mreža bila decentraliziranija i kako bi raspodjela nagrada bila pravedna. Sigurnost je povećana zato jer je gotovo nemoguće provesti neki napad. Napadaču bi trebali privatni ključevi od sudionika u procesu koji su založili više od 60 % od uloženih sredstava kroz dva dana. Sredstva koja su korisnici založili su blokirana za vrijeme njegovog sudjelovanja u procesu, a ponovo dobiva pristup njima sljedeći dan ako je iskreno sudjelovao. U suprotnom, ostaje bez založenih sredstava

koja dobiva sudionik koji je uočio i dokazao zlonamjerno djelovanje. Korisnici koji su odabrani da budu sudionici su poznati unaprijed, a time korisnici postaju ranjiviji [70]. Primjeri uloga korisnika koji žele sudjelovati u procesu te odabira prikazan je na slici ispod.



Slika 4.4.1. Primjer odabira sudionika [70]

Period za koji se biraju sudionici su epohe te se traže korisnici koji će stvarati blokove u jednoj epohi. Za blok na određenoj visini odabire se sudionik koji će stvoriti blok na toj visini, tada se kaže da je to predlagatelj bloka na toj visini [71]. Novu transakciju svaki čvor provjerava te ju, ako je ispravna, dodaje na popis transakcija koje nisu odbačene ili dodane u lanac. Prije stvaranja grupe transakcija predlagatelj bloka ponovo provjerava transakcije kako bi osigurao da su u grupi samo ispravne transakcije [72]. Sudionici za određeni blok mogu poslati poruku potvrde ili poruku za preskakanje bloka. Svaki blok ima visinu te će biti prihvaćen ako je njegova visina za jedan veća od visine prethodnog bloka te ako je dobivena potvrda od sudionika epohe koji su zajedno založili više od 2/3 ukupnih založenih sredstava za trenutnu epohu, a u određenim slučajevima i za sljedeću epohu [71]. Kako bi se povećala efikasnost obrade, sudionici i transakcije iz bloka se raspoređuju u grupe. Grupi sudionika se dodjeljuje grupa transakcija te sudionici obrađuju samo one transakcije za koje su zaduženi. Sudionik tada ne mora preuzimati cijeli blok, već samo one podatke za koje je njegova grupa odgovorna [73]. Opisana tehnologija zove se Nightshade. Treba napomenuti da je još uvijek u razvoju, a zadnja faza će biti završena 2023. godine. Njome će mogući broj transakcija po sekundi biti značajno veći, ali i mreža će biti otvorenija za sudionike u procesu ostvarivanja konsenzusa. Zbog korištenja ove tehnologije, povećanje broja korisnika mreže neće smanjiti njenu učinkovitost. Korištenjem ove tehnologije sudionici neće morati koristiti skupi hardver, kao što je to slučaj kod Ethereuma. Nightshade pridonosi i sigurnosti mreže te ju dovodi na vrlo visoku razinu [74]. Na slici 4.4.2. prikazan je primjer Nightshade tehnologije. *Chunk* je jedna grupa transakcija koja se dodjeljuje grupi sudionika [73].



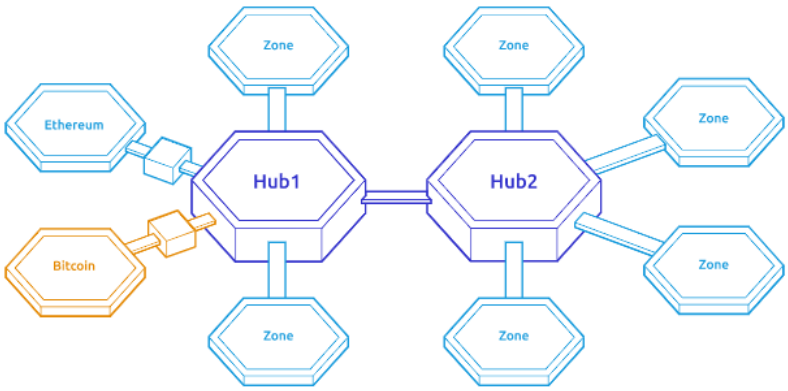
Slika 4.4.2. Nightshade [73]

Za interakciju sa Near *blockchainom* može se koristiti NEAR REST API SERVER. Pomoću njega mogu se razvijati pametni ugovori, izrađivati i prenositi NFT-ovi, a postoje i razne druge mogućnosti [75]. Također, postoji i Near CLI sučelje za interakciju sa *Nearom* preko terminala koji će biti opisan. Prije izrade NFT-a potrebno je razviti i pokrenuti pametni ugovor koji će biti korišten za izradu NFT-a. Za NFT se kod izrade definira njegov identifikator, vlasnik, meta-podaci te raspodjela tantijema [76]. Meta-podaci specificiraju naziv, opis, poveznicu do slike ili videa NFT-a, npr. u IPFS memoriji, broj kopija i razne druge parametre [77]. Korisnici imaju mogućnost izrade kolekcije NFT-ova. Kolekcija je istovremena izrada specificiranog broja NFT-ova koji će imati iste meta-podatke, ali različite identifikatore kako bi svaki od njih i dalje bio jedinstven [76]. NFT-ovi se definiraju prema NEP-171 standardu [76], a njegovi meta-podaci prema NEP-177 standardu [77].

4.5. Cosmos

Cosmos je sustav nezavisnih međusobno povezanih *blockchainova* s fokusom na programere koji sada za svoje decentralizirane aplikacije mogu koristiti vlastiti *blockchain* stvoren baš za tu svrhu. Tada programer definira vlastita pravila rada *blockchaina*. Performanse će biti puno bolje jer transakcije u *blockchainu* rade samo korisnici decentralizirane aplikacije za koju je *blockchain* i stvoren pa neće biti predugog čekanja na potvrdu transakcije, kao što je to moguće na drugim *blockchainovima*. Cosmos se još naziva Internet of Blockchains, a zasniva se na tehnologiji Tendermint Core [78]. Tendermint BFT omogućuje obradu blokova u jednoj sekundi te obradu tisuće transakcija u sekundi [79]. U centru Cosmos mreže nalazi se Cosmos Hub, prvi *blockchain* nastao na Cosmosu. Popularni Binance Chain i Crypto.org su *blockchainovi* u sklopu Cosmos mreže. Cosmos Hub ima vlastiti *token* ATOM [78], s ciljem da u budućnosti ne podržava samo tu kripto valutu, već više njih [80]. *Blockchainovi* unutar Cosmos mreže stvaraju se koristeći Cosmos

SDK (*software development kit*) otvorenog koda, a mehanizmi ostvarivanja konsenzusa koje mogu koristiti su javni *Proof-of-Stake* ili *Proof-of-Authority* [81]. Za međusobno povezivanje *blockchainova* unutar mreže koristi se Inter-blockchain communication (IBC) protokol koji omogućava razmjenu podataka između *blockchainova* [82]. Zbog mogućnosti postojanja velikog broja *blockchainova* u Cosmos mreži, nemoguće je očekivati da će svaki *blockchain* biti povezan sa svim ostalim *blockchainovima* jer to zahtjeva ogroman broj veza. Da bi se smanjio broj veza koristi se modularna arhitektura sa dvije klase modula, a to su središte i zona. Radi tako da postoji jedno ili više središta mreže (npr. Cosmos Hub) te veliki broj zona. Središta povezuju zone te zone pomoću središta mogu međusobno komunicirati, vršiti transakcije. Svaki *blockchain* koji postoji u Cosmos mreži je jedna zona te je svaka zona povezana sa određenim središta. Na Cosmos mrežu se može povezati i *blockchain* koji se ne zasniva na Tendermint Core tehnologiji, npr. Bitcoin, što znači da i Bitcoin može biti jedna zona. Hub provjerava transakcije između zona [79]. Primjer arhitekture Cosmos mreže se nalazi na slici ispod.

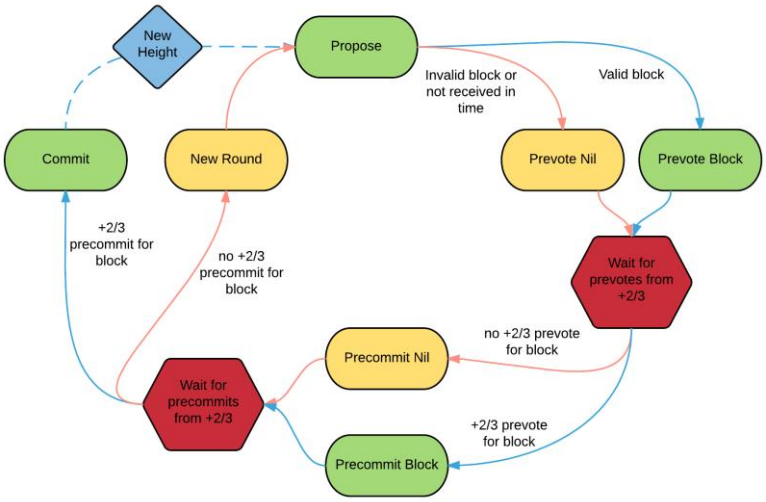


Slika 4.5.1. Primjer arhitekture Cosmos mreže [79]

Velika prednost Cosmos mreže su vrlo niske naknade, a iznose $0.01, što je trenutno tek nešto više od 0 HRK (0.074 HRK) [83]. Cosmos Hub *validator* može birati u kojem *tokenu* ili kombinaciji *tokena* želi primati naknade, a tečaj zamjene *tokena* proizvoljno zadaje. *Validator* ima slobodu odabira transakcije koju želi obraditi, dok god potrebni računalni resursi bloka ne prelaze postavljenu granicu. Određeni dio naknada za obradu transakcija se vraća među zalihe mreže kako bi se povećale vrijednost i sigurnost mreže. Korisnici koji otkriju da je određeni korisnik kompromitiran mogu to prijaviti. U tom slučaju će kompromitiran korisnik postati neaktivan, bit će mu oduzeta određena količina sredstava s računa. Dio oduzetih sredstava će dobiti korisnik koji je prijavio kompromitiranost kao nagradu, a ostatak sredstava kompromitirani korisnik može vratiti koristeći ključ za oporavak. Dodatno, *validator* može ostati bez dijela sredstava ako bude

nedostupan, tj. ne sudjeluje u procesu, duže od nekog zadanog vremena. U tom slučaju će *validator* također postati neaktivan [84].

U Tendermint mehanizmu ostvarivanja konsenzusa svaki čvor dobiva određeno pravo na glasanje, a može poprimiti vrijednost 0 ili pozitivnu. Čvorovi sa pozitivnim pravom su *validatori* te će moći sudjelovati u procesu ostvarivanja konsenzusa. Pravo čvora na sudjelovanje se mijenja ovisno o *blockchainu*. Čvorovi koji ne mogu biti *validatori* mogu prenijeti određeni broj sredstava *validatoru* kako bi dobili dio njegove nagrade, ali time riskiraju gubitak uloženog ukoliko se *validator* kompromitira ili djeluje zlonamjerno. Ti čvorovi se zovu *delegatori*. *Validatori* i *delegatori* imaju pravo glasa i kod uvođenja promjena u sustav. Protokol zahtijeva određeni broj *validatora*, a svaki *validator* će biti predstavljen javnim ključem. Proces ostvarivanja konsenzusa se odvija u rundama. Svaka runda ima voditelja koji predlaže blok. Voditelj se odabire proporcionalno pravu na glasanje. Potom *validatori* u dvije faze glasanjem odlučuju hoće li blok biti prihvaćen. Ako je u obje faze više od 2/3 *validatora* glasalo za taj blok, blok će biti dodan. U suprotnom, prelazi se na sljedeću rundu. Ako se dogodi da *validator* ne da svoj glas u vremenu u kojem ga je trebao dati, *validator* će biti privremeno deaktiviran te u tom periodu neće moći sudjelovati u procesu. U tom periodu pravo na sudjelovanje nasljeđuju delegatori deaktiviranog *validatora*, ali njihovi glasovi možda budu poništeni [84]. Proces je prikazan na slici ispod.



Slika 4.5.2. Proces ostvarivanja konsenzusa u Tendermint mehanizmu [85]

U Cosmos mreži predložen je i implementiran NFT modul ADR 43. Programeri ne moraju upotrijebiti tu implementaciju već kod razvoja vlastitog *blockchaina* mogu implementirati i vlastiti NFT modul koji više odgovara njihovim potrebama. NFT modul, kao i svi ostali moduli, nalazi se unutar Cosmos SDK-a te se onda kod programiranja *blockchaina* može i konfigurirati NFT modul tako da najbolje odgovara potrebama *blockchaina*. Velika prednost NFT modula je mogućnost korištenja na različitim *blockchainovima* unutar Cosmos mreže korištenjem spomenutog IBC protokola. Zadana implementacija NFT modula omogućuje izradu NFT-a, prenošenje i praćenje vlasništva, uništavanje NFT-a te pretraživanje NFT-ova i podataka o njima. Modul se sastoji od NFT klase i objekta koji predstavlja NFT, a povezan je sa NFT klasom. U NFT klasi se definira njen identifikator, naziv, opis, simbol i poveznica na meta-podatke klase, itd. Objekt NFT-a i NFT klasa su povezani tako što objekt sadrži identifikator klase. Neki od atributa koji se definiraju u objektu su identifikator objekta i poveznica na meta-podatke NFT-a [86]. Korisnici koji samo žele izraditi NFT na nekom od postojećih *blockchainova* mogu isto učiniti koristeći Stargaze dokumentaciju. Nakon izrade NFT će biti vidljiv u *marketplaceu* na Stargaze *blockchainu* unutar Cosmos *blockchain* mreže [87].

5. TESTIRANJE

Nakon detaljnijeg opisa svake *blockchain* mreže koja će biti korištena u ovom projektu, prijeđimo na provođenje testiranja izrade nezamjenjivih *tokena* na svakoj od njih. Opisi parametara se mogu pronaći u dokumentaciji koja je korištena za izradu.

5.1. Ethereum

Testiranje je provedeno na Goerli Testnet *blockchainu* te je provedeno prema Ethereum dokumentaciji. Potrebno se povezati na Ethereum *blockchain*, stvoriti Ethereum račun i napuniti ga testnim sredstvima. Zatim slijede inicijalizacija projekta te pisanje, *compile* i *deploy* pametnog ugovora. Nakon *deploya* pametnog ugovora postavljaju se meta-podaci NFT-a te se izrađuje NFT. Nakon uspješne izrade NFT se prikazuje u novčaniku. Inicijalna konfiguracija pametnog ugovora definirala je da se pametni ugovor pohrani na Ropsten *blockchain* te je konfiguracija izmijenjena kako si se *deploy* pametnog ugovora radio na Goerli *blockchain*. Inicijalni meta-podaci NFT-a opisivali su životinju [88, 89, 90]. Spomenuti inicijalni podaci, kao i nekoliko ostalih, su izmijenjeni kako bi odgovarali projektu. Izmjene u datotekama iz dokumentacije prikazane su u nastavku.

Prilikom inicijalizacije projekta [88] podaci su izmijenjeni kako bi bolje odgovarali zadatku ovog rada, a izmjene su prikazane ispod.

```
"name": "ethernft",
"version": "1.0.0",
"description": "Mint test on Ethereum"
```

Slika 5.1.1. Informacije o projektu

U datoteci *RitehNFTContract.sol* [88] koja sadrži programski kod pametnog ugovora promijenjen je naziv ugovora u RitehNFTContract te je konstruktoru *ERC721* poslana druga vrijednost naziva pametnog ugovora, kako bi odgovarao radu, pa on sada izgleda ovako:

```
constructor() ERC721("RitehNFT", "NFT") {}
```

Slika 5.1.2. Konstruktor ERC721

Datoteka *hardhat.config.js*, tj. konfiguracija Hardhat alata za razvoj pametnih ugovora na Ethereum *blockchainu* [88] nalazi se na slici ispod.

```
require('dotenv').config();
require("@nomiclabs/hardhat-ethers");
const { API_URL, PRIVATE_KEY } = process.env;
module.exports = {
  solidity: "0.8.9",
  defaultNetwork: "goerli",
   networks: {
      hardhat: {},
      goerli: {
         url: API_URL,
         accounts: [`0x${PRIVATE_KEY}`]
      }
   }
};
```

Slika 5.1.3. Datoteka hardhat.config.js

Izmjene su morale biti učinjene zato što se nezamjenjivi token izrađuje na Goerli Testnet *blockchainu*. Varijabla API_KEY je ključ za pristup Alchemy API-ju, a PRIVATE_KEY je privatni ključ Metamask novčanika. Zbog sigurnosti njihove vrijednosti neće biti prikazane. Sljedeći korak je razvoj pametnog ugovora koji je umjesto „MyNFT“ nazvan „RitehNFTContract“ [88].

Programski kod za slanje ugovora na *blockchain* (eng. *deploy*) [88] izmijenjen je samo kako bi tražio pametni ugovor pravog naziva.

```
const Contract = await ethers.getContractFactory("RitehNFTContract")
```

Slika 5.1.4. Novi argument funkcije getContractFactory()

Deploy pametnog ugovora trajao je 66 sekundi te je pohranjen na adresu 0x68a45646d763105d2033C44f26e6AC633c58c8c1.

Meta-podaci nezamjenjivog *tokena* [89] postavljeni su na sljedeći način:

```
{
  "description": "Testing NFT minting on Goerli.",
  "image": "ipfs://QmasiwuWvmRkKbUxsQb6R1Ap5uwa4pchGSQXpMNuZBcS5g",
  "name": "RitehNFT"
}
```


Slika 5.1.5. Meta-podaci nezamjenjivog tokena

Image atribut sadrži *hash* slike NFT-a u IPFS memoriji, a za pohranu je korišten alat Pinata. Definirani su i naziv i opis nezamjenjivog *tokena* [89].

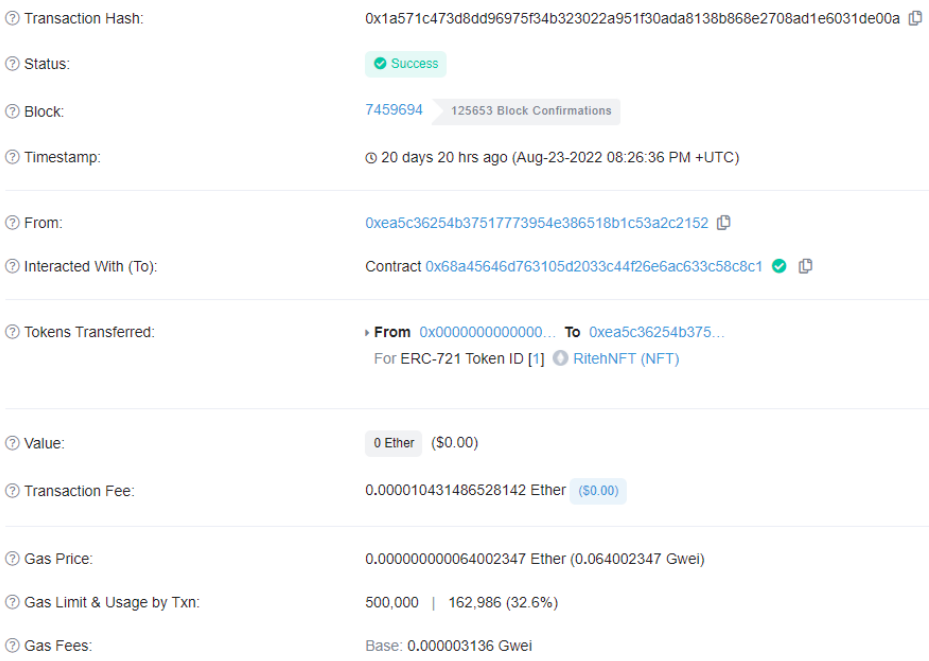
U datoteci *MINT-NFT.js* [89] napravljene su dvije izmjene, a to su:

```
const contract = require("../artifacts/contracts/RitehNFTContract.sol/RitehNFTContract.json")
const contractAddress = "0x68a45646d763105d2033C44f26e6AC633c58c8c1"
```

Slika 5.1.6. Izmjene u datoteci MINT-NFT.js

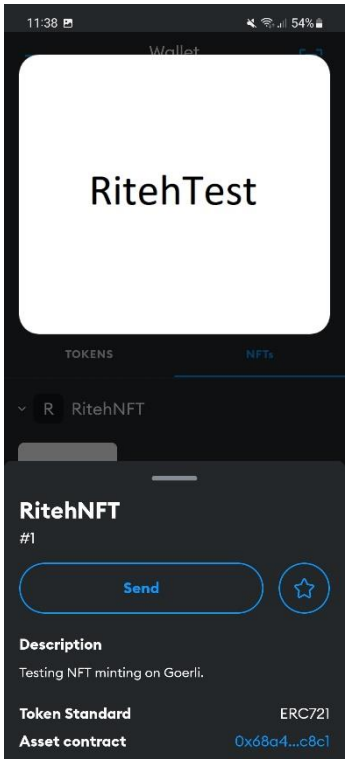
Prva izmjena na napravljena zbog već spomenutih izmjena u nazivu pametnog ugovora kako bi se dohvatilo sučelje za interakciju s ugovorom. U sljedećoj liniji je definirana adresa pametnog ugovora koji je ranije u radu pohranjen na *blockchain* [89].

Meta-podatke NFT-a je potrebno pohraniti u IPFS memoriju. Sada je sve spremno za izradu nezamjenjivog *tokena* na Goerli *blockchainu* te sa dobivenim *hashom* meta-podataka u IPFS memoriji možemo pokrenuti izradu [89]. Od pokretanja programskog koda do pojave transakcije na Goerli Exploreru prošlo je 20-ak sekundi, a detalji su prikazani na slici 5.1.7.



Slika 5.1.7. Detalji transakcije [91]

Izrađeni nezamjenjivi *token* vidljiv je i u MetaMask novčaniku prateći upute iz dokumentacije [90].



Slika 2: NFT u novčaniku

5.2. Algorand

Programski kod za izradu nezamjenjivog *tokena* na Algorand Testnetu pisan je u Node.Js programskog jeziku. Prilikom pisanja korišten je službeni predložak programskog koda za izradu nezamjenjivog *tokena* sa potrebnim paketima [92]. Informacije o paketu mogu se izmijeniti po uzoru na izmjene koje su učinjene kod izrade na Ethereum *blockchainu*. Za razliku od izrade na Ethereum *blockchainu,* ovdje potreban programski kod stane u jednu datoteku. Ta datoteka je u predlošku nazvana *index.js* te će određeni dio koda iz te datoteke biti iskorišten u novoj datoteci unutar istog paketa. Na početku je bilo potrebno konfigurirati Sandbox server. Sandbox server može biti pokrenut na vlastitom računalu ili se može povezati na udaljeni server. Testirano je oboje te oboje radi. Na slici 5.2.1. prikazana je konfiguracija udaljenog servera.

```
// sandbox
const token = "2f3203f21e738a1de6110eba6984f9d03e5a95d7a577b34616854064cf2c0e7b";
const server = "https://academy-algod.dev.aws.algodev.network";
const port = 443;
```

Slika 5.2.1. Konfiguracija sandboxa

Slijedi definiranje računa na kojem će biti izrađen nezamjenjivi *token*. Algosdk omogućuje izradu računa u programskom kodu [92], ali korisnije je koristiti jedan račun nego svaki nezamjenjivi *token* izraditi na novom računu.

U prvoj liniji je potrebno definirati frazu od 25 riječi vlastitog računa te se pomoću nje dolazi do samog računa, njegove adrese i privatnog ključa. Iz sigurnosnih razloga, fraza računa korištenog u radu nije prikazana.

```
let account1_mnemonic = '';
var recoveredAccount1 = algosdk.mnemonicToSecretKey(account1_mnemonic);
```

Slika 5.2.2. Definiranje računa

Meta-podaci nezamjenjivog *tokena* su prikazani na slici 5.2.3., a definirani su prema meta-podacima iz predloška, u datoteci *NFT/metadata.json* [92].

```
{
    "name": "RitehNFT",
    "description": "Testing NFT mint on Algorand",
    "image": "https://gateway.pinata.cloud/ipfs/QmasiwuWvmRkKbUxsQb6R1Ap5uwa4pchGSQXpMNuZBcS5g",
    "image_integrity": "sha256-JjmioczKeFgMMgwpI0kPW1jXaRmV4DQSeo7i+5YwdwI=",
    "properties": {
        "simple_property": "Test"
    }
}
```

Slika 5.2.3. Meta-podaci nezamjenjivog tokena

Parametar *image_integrity* sadrži *hash* slike nezamjenjivog *tokena*. Kao *simple_property* svojstvo mogla bi se definirati vrsta studentskog digitalnog *bedža*, u kontekstu ovog projekta. Također, definirani su naziv, opis te poveznica do slike nezamjenjivog *tokena*.

Na Algorand *blockchainu* se za definiranje *asseta* koristi Algorand Standard Assets standard te će sada biti definirani njegovi parametri.

```
let params = await algodclient.getTransactionParams().do();
let note =  undefined; // arbitrary data to be stored in the transaction; here, none is stored
let addr = recoveredAccount1.addr;
// Whether user accounts will need to be unfrozen before transacting
let defaultFrozen = false;
// integer number of decimals for asset unit calculation
let decimals = 0;
// total number of this asset available for circulation
let total = 1;
// Used to display asset units to user
let unitName = "RitehNFT";
// Friendly name of the asset
let assetName = "RitehNFT@arc3";
// Optional string pointing to a URL relating to the asset
let assetURL = 'https://gateway.pinata.cloud/ipfs/QmbR4MDGPTFdByJkS2u1y1vvTtatovFhbsyonVVEqFEHQS';
// Optional hash commitment of some sort relating to the asset. 32 character length.

const pathToMetadata = __dirname + '/nft/metadata.json';
const metadata = (await fs.readFile(pathToMetadata));

const hash = crypto.createHash('sha256');
hash.update(metadata);
let assetMetadataHash = new Uint8Array(hash.digest());

let manager = recoveredAccount1.addr;
let reserve = recoveredAccount1.addr;
let freeze = recoveredAccount1.addr;
let clawback = recoveredAccount1.addr;
```

Slika 5.2.4. Parametri nezamjenjivog tokena

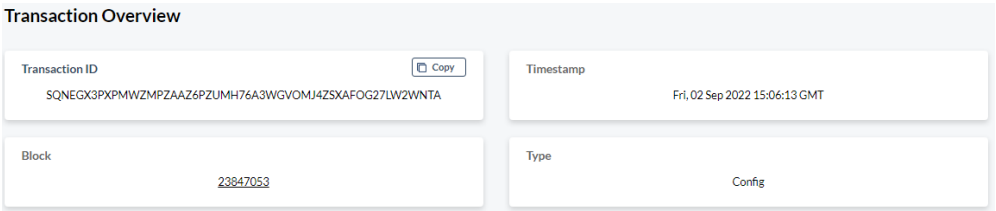
Pošto se definira nezamjenjivi *token*, parametrima *decimals* i *total* su postavljene vrijednosti 0 i 1 kako bi se pokazalo da se radi o nezamjenjivom *tokenu*. Nazivi jedinice i *asseta* su postavljeni kako bi odgovarali projektu. Parametar *assetURL* sadrži poveznicu do meta-podataka u IPFS memoriji. Parametrima *manager*, *reserve*, *freeze* i *clawback* definiraju se adrese računa koji će dobiti određenu kontrolu nad nezamjenjivim *tokenom*. Vrijednost svih parametara je adresa kreatora nezamjenjivog *tokena*, čime on dobiva potpunu kontrolu. U budućnosti se prilikom prijenosa nezamjenjivog *tokena* kontrola može dati primatelju, a moguće je nekom od tih parametara kao vrijednost zadati prazan *string* („“) kako bi onemogućili tu funkcionalnost [51].

Nakon što su definirani parametri, sve je spremno za definiranje transakcije, njeno potpisivanje, slanje na *blockchain* te čekanje potvrde.

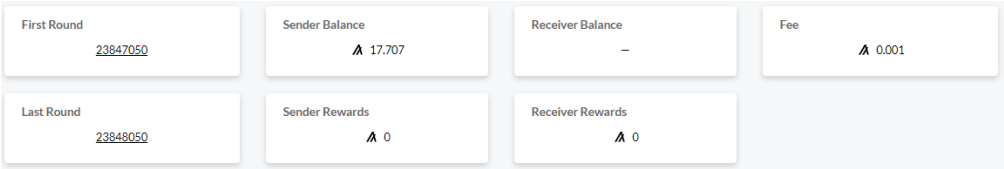
```
let txn = algosdk.makeAssetCreateTxnWithSuggestedParams(
    addr, note, total, decimals, defaultFrozen, manager, reserve,
    freeze, clawback, unitName, assetName, assetURL,
    assetMetadataHash, params);

let rawSignedTxn = txn.signTxn(recoveredAccount1.sk)
let tx = (await algodclient.sendRawTransaction(rawSignedTxn).do());

let assetID = null;
// wait for transaction to be confirmed
const conf = await algosdk.waitForConfirmation(algodclient, tx.txId, 4);
```

Slika 5.2.5. Stvaranje transakcije, potpis, slanje i potvrda

Prije pokretanja potrebno je provjeriti ima li sredstava na definiranom Testnet računu te, ako nema, uplatiti pomoću službenog davatelja Testnet sredstava [93]. Od početka izvršavanja do pojave transakcije na Algorand blochchainu proteklo je manje od pet sekundi. Detalji o transakciji i *assetu* su vidljivi u Algorand Exploreru.

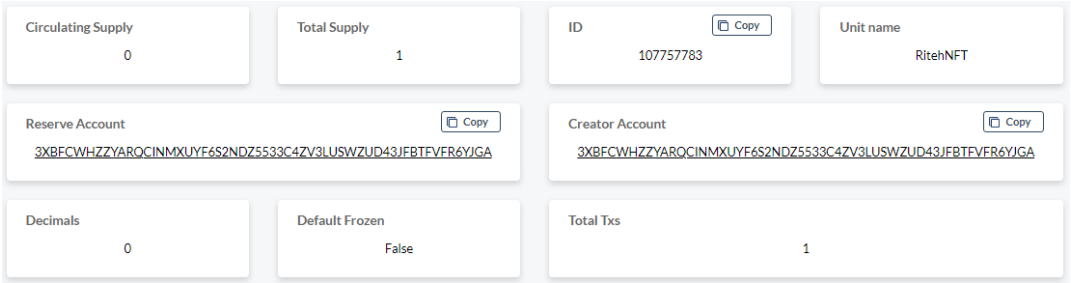


Slika 5.2.6. Detalji o transakciji 1/2 [94]

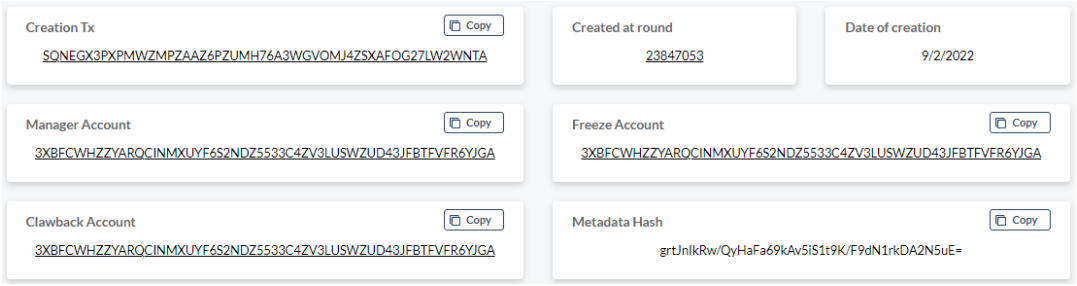


Slika 5.2.7. Detalji o transakciji 1/2 [94]

Među detaljima o transakciji i *assetu* informacije se uglavnom ponavljaju te su ti podaci prikazani samo iz detalja o *assetu*.

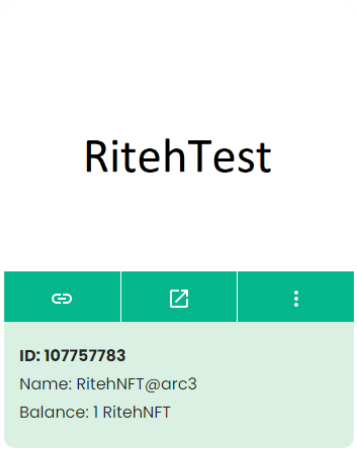


Slika 5.2.8. Detalji o assetu 1/2 [95]



Slika 5.2.9. Detalji o assetu 2/2 [95]

Iz detalja je vidljivo kako je programski kod dao uspješan rezultat te svi parametri imaju one vrijednosti koje su im u kodu i postavljene. Kako bi se testirala ispravnost poveznice do meta-podataka potrebno je provjeriti da li je u novčaniku vidljiv novostvoreni *asset*, za što je korišten Algodesk. Pritiskom na karticu *NFT collection* vidljiv je stvoreni nezamjenjivi *token*.



Slika 5.2.10. Izrađeni nezamjenjivi token

Također, moguće je pregledati i njegove meta-podatke.

Slika 5.2.11. Metapodaci izrađenog nezamjenjivog tokena u novčaniku

Može se potvrditi da je nezamjenjivi *token* uspješno stvoren te da su njegovi meta-podaci uspješno postavljeni.

5.3. Cardano

Za izradu nezamjenjivog *tokena* na Cardano *blockchainu* korišten je Tangocrypto API koji služi za interakciju sa Cardano *blockchainom*, bez potrebe da računalo sadrži potpuni Cardano čvor. Tijekom izrade korištena je dokumentacija spomenutog API-ja [96, 97, 98]. Kako bi se API mogao koristiti nužno je izraditi korisnički račun za API te na njemu stvoriti aplikaciju čime se dobije

ključ za korištenje API-ja i identifikacijski *hash* aplikacije. Svaki zahtjev API-ju zahtjeva definiranje ta dva podatka te bez njih zahtjev ne prolazi. Za slanje zahtjeva korišten je Linux terminal.

Prvi korak u izradi nezamjenjivog *tokena* je izrada kolekcije nezamjenjivih *tokena*, a to se radi na sljedeći način:

```
curl --request POST \
  --url https://cardano-testnet.tangocrypto.com/<app_id>/v1/nft/collections \
  --header 'Content-Type: application/json' \
  --header 'x-api-key: ' \
  --data '{
  "name": "Riteh Test Collection",
  "description": "Collection for testing NFT mint on Cardano",
  "payout_address":
"addr_test1qzjcuyyv9mxgaqyk7j9ykt5mjza9gpd2sv6u57xwkeap8q387yu6f7pwtux6sxhqwu
m46geacwrjngsgwhgq8yxtl42s5w0m7q",
  "policy": {
    "lock": true,
    "lock_time": "2022-09-20"
  },
  "metadata": {
    "name": "<name>",
    "asset_name": "<asset_name>",
    "description": "<description>",
    "attributes": {
      "collection": "Riteh Test Collection",
      "artist": "RBT"
    },
    "version": "1.0"
  }
}'
```

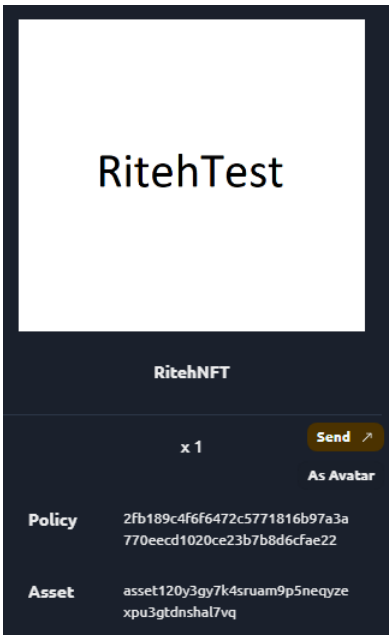
Prikazano je kako se definiraju kolekcija i skripta pravila, a detaljni opisi svih parametara nalaze se u dokumentaciji [96]. Parametri <*app_id*> i *api-key* iz sigurnosnih razloga nisu prikazani. Zahtjev je dao rezultat za nešto manje od pola sekunde te je tada API započeo postavljanje slike i sadržaja u IPFS memoriju. Između ostalog dobiven je identifikacijski *hash* koji se koristi u sljedećim koracima, a prvo kod stvaranja nezamjenjivog *tokena*.

```
curl --request POST \
 --url https://cardano-testnet.tangocrypto.com/<app_id>/v1/nft/collections/<collection_id>/tokens
\
 --header 'Content-Type: application/json' \
 --header 'x-api-key: ' \
 --data '{
 "tokens": [
  {
   "asset_name": "RitehNFT",
   "name": "RitehNFT",
   "description": "Testing NFT mint on Cardano",
   "image": "",
   "metadata_attributes": [
    {
     "tag": "Type",
     "value": "Test"
    }
   ]
  }
 ]
}'
```

U ovom zahtjevu je stvoren nezamjenjivi *token* te su definirani njegovi meta-podaci. Osim standardnih podataka o nazivu i opisu, *image* parametar u ovom slučaju nije poveznica na sliku, već je to base64 *hash*. Zbog dužine nije prikazan. Opis svih parametara nalazi se u dokumentaciji [97]. Zbog sigurnosti nisu prikazani parametri *<app_id>*, *<collection_id>* i *api-key*. Međutim, u ovom slučaju stvaranje nezamjenjivog *tokena* ne znači i izrađivanje („mintanje“), izrađen će biti nakon prodaje pa sada slijedi pokretanje prodaje.

```
curl --request POST \
 --url https://cardano-testnet.tangocrypto.com/<app_id>/v1/nft/collections/<collection_id>/sales \
 --header 'Content-Type: application/json' \
 --header 'x-api-key: ' \
 --data '{
 "type": "random",
 "price": 6000000,
 "reservation_time": 300
}'
```

Moguće je pomoću identifikacijskog stringa specificirati nezamjenjivi *token* za prodaju, tj. koristiti vrstu prodaje „fixed“, ali radi jednostavnosti je korištena vrsta „random“. Vrsta prodaje „random“ znači da će se za prodaju nasumično odabrati jedan nezamjenjivi *token* iz kolekcije. Pošto trenutna kolekcija sadrži jedan nezamjenjivi *token*, on će biti i odabran za prodaju. Cijena je postavljena na 6.000000 ADA. Dodatno, definirano je koliko će NFT vremenski biti rezerviran za korisnika koji započne kupnju [98]. Zahtjev je izvršen za otprilike pola sekunde te su kao odgovor dobivene informacije o prodaji sa adresom za plaćanje. Sada kada je pokrenuta prodaja nezamjenjivog *tokena* dovoljno je iz Nami novčanika poslati 6.000000 ADA na spomenutu adresu za plaćanje. Nakon potvrde transakcije nezamjenjivi *token* je za oko minutu i pol bio izrađen i vidljiv u novčaniku.



Slika 5.3.1. Nezamjenjivi token u Nami novčaniku

Iako je izrađeni nezamjenjivi *token* vidljiv u novčaniku i Tangocrypto grafičkom sučelju, Cardanoscan Testnet Explorer nema tu transakciju, pomoću API-ja se, u slučaju potrebe, može doći do informacija o njoj.

5.4. Near

Za izradu nezamjenjivog *tokena* na Near *blockchainu* korišteno je *near-cli* Near sučelje komandne linije, a potrebne naredbe nalaze se u dokumentaciji [99]. U preuzetom primjeru izmijenjen je programski kod pametnog ugovora u datoteci *nft/src/lib.rs*, točnije meta-podaci ugovora u funkciji *new_default_meta*. Ispod je prikazano kako su sada definirani meta-podaci.

```
#[init]
pub fn new_default_meta(owner_id: AccountId) -> Self {
    Self::new(
        owner_id,
        NFTContractMetadata {
            spec: NFT_METADATA_SPEC.to_string(),
            name: "Riteh NFT Contract".to_string(),
            symbol: "RBT".to_string(),
            icon: Some(DATA_IMAGE_SVG_NEAR_ICON.to_string()),
            base_uri: None,
            reference: None,
            reference_hash: None,
        }
    )
}
```

Slika 5.4.1. Meta-podaci pametnog ugovora

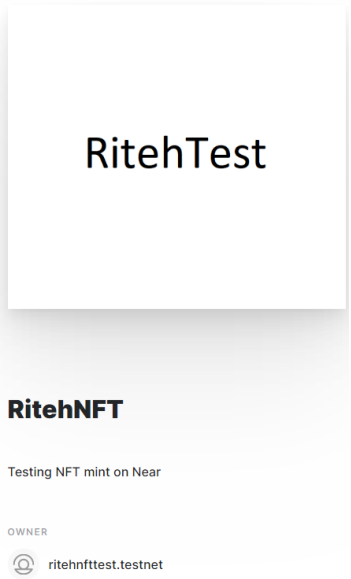
Naziv i simbol imaju vrijednosti koje više odgovaraju projektu. Sada je sve spremno za izvršavanje naredbi iz dokumentacije [99].

Deploy pametnog ugovora trajao je oko 18.5 sekundi, a inicijalizacija pametnog ugovora sa ranije definiranim meta-podacima oko 17 sekundi.

U naredbi kojom se izrađuje nezamjenjivi *token* [99] izmijenjen je dio koji označava njegove meta-podatke te su oni sada definirani na sljedeći način:

```
near call $ID nft_mint '{"token_id": "1", "receiver_id": "'$ID'", "token_metadata": { "title":
"RitehNFT", "description": "Testing NFT mint on Near", "media":
"https://gateway.pinata.cloud/ipfs/QmasiwuWvmRkKbUxsQb6R1Ap5uwa4pchGSQXpMNuZBcS5g",
"copies": 1}}' --accountId $ID --deposit 0.1
```

Izrada je trajala otprilike 16 sekundi te je nakon nje bilo moguće vidjeti novoizrađeni nezamjenjivi *token* u novčaniku.



Slika 5.4.2. Nezamjenjivi token u Near Testnet novčaniku

Time je dokazano da je kod izvršavanja naredbe definirana ispravna poveznica do slike. U novčaniku se ne mogu pregledati meta-podaci, ali mogu se u Near Testnet Exploreru.

Prema slici se vidi da su meta-podaci uspješno definirani.


```
{
  "token_id": "1",
  "receiver_id": "ritehnfttest.testnet",
  "token_metadata": {
    "title": "RitehNFT",
    "description": "Testing NFT mint on Near",
    "media": "https://gateway.pinata.cloud/ipfs/QmasiwuWvmRkKbUxsQb6R1Ap5uwa4pchGSQXpMNuZBcS5g",
    "copies": 1
  }
}
```


Slika 5.4.3: Meta-podaci nezamjenjivog tokena [100]

5.5. Cosmos

Nezamjenjivi *token* izrađen je na Elgafar *blockchainu*, Stargaze Testnet *blockchainu u* sklopu Cosmos *blockchain* mreže, a za izradu je korišten paket alata za izradu nezamjenjivih *tokena* na Stargaze *blockchainu* naziva *stargaze-tools* te službena dokumentacija za izradu [101, 102, 103, 104, 105, 106, 107].

Prvi korak je pokretanje projekta izrade [101]. Sljedeći korak je postavljanje projekta prema dokumentaciji [102]. Nakon postavljanja projekta slijedi učitavanja slike nezamjenjivog *tokena* i meta-podataka na neku od udaljenih vrsta pohrane, npr. IPFS. Radi jednostavnosti je korištena naredba koja uzima datoteke iz direktorija *images* i *metadata* te ih postavlja u IPFS memoriju na dvije zasebne lokacije. Točnije, korištena je naredba koja pomoću NFT.storage API-ja postavlja datoteke u IPFS memoriju. Detaljni koraci koje je potrebno izvršiti nalaze se u dokumentaciji [103, 104]. Meta-podaci su definirani na sljedeći način:


```
{
    "attributes":[
        {
            "trait_type":"Type",
            "value":"Test"
        }
    ],
    "description":"Testing NFT mint on Elgafar",
    "image":"ipfs://bafybeic3dmejphrejcjfehenz4vyqm5makbtmttn3atse34orivpgaelfy/images/1.png",
    "name":"RitehNFT"
}
```


Slika 5.5.1. Meta-podaci nezamjenjivog tokena

Definirani su naziv, opis, IPFS *hash* do slike te se mogu definirati razni atributi. Kao vrijednost atributa *Type* može se definirati vrsta digitalnog studentskog bedža unutar Riteh Blockchain Teama [103].

Konfiguracija koja će biti korištena za izradu kolekcije, pametnog ugovora te nezamjenjivog *tokena* nalazi se u datoteci *config.js*. Na slici 5.5.2. je prikazano kako je definirana kolekcija.

```
name: 'RitehNFT',
symbol: 'RBT',
description: 'Testing NFT mint on Elgafar',
image: 'ipfs://bafybeic3dmejphrejcjfehenz4vyqm5makbtmttn3atse34orivpgaelfy/images/1.png',
```

Slika 5.5.2. Konfiguracija kolekcije

Image parametar predstavlja IPFS *hash* slike koja će predstavljati cijelu kolekciju. U ovom projektu kolekcija sadrži jedan nezamjenjivi *token* pa je slika tog *tokena* i slika kolekcije. Definirani su još naziv, opis i simbol kolekcije [105].

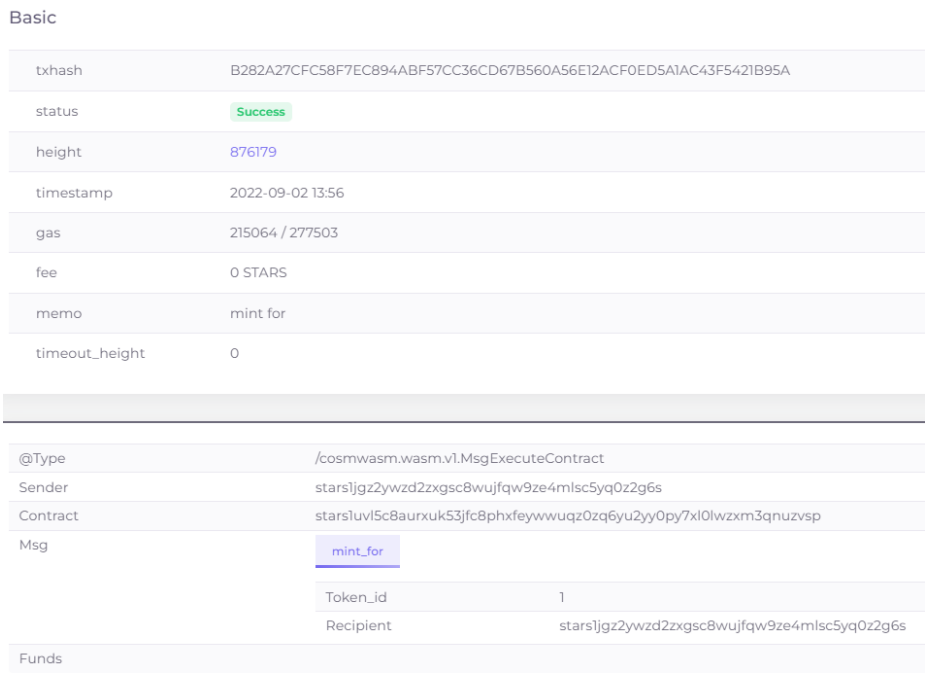
Prije početka izvršavanja sljedećih naredbi iz dokumentacije [105] potrebno je u datoteci *config.js* definirati pametni ugovor, što je prikazano ispod.

```
// The base URI to be used to programatically mint tokens
baseTokenUri: 'ipfs://bafybeida3v4jyhdmec7i4lwivn3s7wi554wqueh5ix3pbwj7ugs6yjigdu/galaxyINudsn',
// The number of tokens to mint
numTokens: 1,
// The price (in STARS) for your NFTs (minimum 50 STARS)
unitPrice: 50,
// The max amount of NFTs an address can mint
perAddressLimit: 50,
// The date when the sale goes live
// If whitelist is enabled, only whitelisted addresses will be able to purchase
// startTime in ISO format
startTime: '2022-09-02T11:56:00.000Z',
// The minter contract address
// Get this after running `yarn minter`
minter: 'stars1uvl5c8aurxuk53jfc8phxfeywwuqz0zq6yu2yy0py7xl0lwzxm3qnuzvsp',
// SG721 contract address
// Get this after running `yarn minter`
sg721: 'stars1lt6qyqckmlctgmr462h7fssdtde3qn2sw3sw0p3e2k8ejp6al8msluzv5r',
```

Slika 5.5.3. Konfiguracija pametnog ugovora

U pametnom ugovoru se definira IPFS *hash* do meta-podataka nezamjenjivog *tokena* koji će biti izrađen, broj *tokena*, cijena jednog i broj nezamjenjivih *tokena* koje jedan korisnik može izraditi. Potrebno je definirati i od kada će biti moguće izraditi nezamjenjivi *token* iz te kolekcije. Također, za izradu nezamjenjivog *tokena* potrebno je definirati *minter* adresu pametnog ugovora koja se dobije kao izlaz naredbe za izradu ugovora. Sada je sve spremno za praćenje uputa u dokumentaciji za izradu pametnog ugovora [106] te za izradu nezamjenjivog *tokena* [107].

Izrada kolekcije i pametnog ugovora trajala je otprilike 39 sekundi, a izrada nezamjenjivog *tokena* nešto manje od 24 sekunde. Transakcije su vidljive u Publicawesome Testnet Exploreru, a informacije o transakciji izrade nezamjenjivog *tokena* prikazane su ispod.



Slika 5.5.4. Transakcija izrade nezamjenjivog tokena [108]

Nezamjenjivi *token* se može pregledati na Stargaze Testnet *marketplaceu*.

Slika 5.5.5. Prikaz nezamjenjivog tokena na Stargaze Testnet profilnoj stranici [109]

6. ANALIZA REZULTATA TESTIRANJA

Nakon što je odrađeno testiranje, slijedi analiza rezultata. Rezultati će biti analizirani prema naknadama koje su plaćene u procesu izrade nezamjenjivog *tokena*, iz perspektive jednostavnosti procesa izrade, količina potrošenih računalnih resursa te za resurse plaćene naknade i drugo.

Ako se gleda jednostavnost izrade nezamjenjivog *tokena*, svi korišteni *blockchainovi* imaju opsežnu dokumentaciju za izradu. Na Near *blockchainu* nezamjenjivi *token* je izrađen nakon izvršavanja samo nekoliko naredbi, korištenjem predloška programskog koda. S druge strane, Algorand *blockchainu* ne zahtijeva korištenje pametnog ugovora. *Asset* se definira kao Algorand Standard Asset te se vrijednostima parametara on definira kao nezamjenjivi *token*. Sve to je moguće napraviti u jednoj funkciji programskog koda.

6.1. Plaćene naknade i potrošeni računalni resursi

Važnija stavka po kojoj se rezultati mogu analizirati su naknade za izradu nezamjenjivog *tokena* na pojedinom *blockchainu*. Plaćene naknade su vidljive među detaljima pojedine transakcije. Treba napomenuti da su navedene naknade u testnim *tokenima* koji nemaju stvarnu vrijednost. Za *deploy* pametnog ugovora na Goerli Testnet *blockchain* potrošeno je 2 557 782 jedinica računalnih resursa. Ako je cijena jedne jedinice u trenutku otprilike 0.0000000015 Ether, tada je ukupna naknada za spomenutu količinu jedinica otprilike 0.00384 Ether, taj iznos je dobio rudar koji je obradio transakciju. Uništeno je otprilike 0.000000004 Ether [110]. Za izradu nezamjenjivog *tokena* potrošeno je 162 986 jedinica računalnih resursa. U tom trenutku je cijena jedne jedinice bila oko 0.00000000006 Ether pa je naknada za transakciju iznosila otprilike 0.00001043 Ether. Uništeno je oko0.000000000000003136 Ether [91].

Cijena izrade nezamjenjivog *tokena* na Algorand *blockchain* iznosila je 0.001 ALGO [94], što je i minimalna naknada na tom *blockchainu*. Pošto nema potrebe za korištenjem pametnog ugovora, nema niti naknade za njegov *deploy*, što je svakako prednost.

Za izradu nezamjenjivog *tokena* na Cardano *blockchainu* korišten je Tangocrypto API koji ima minimalnu cijenu od 5.221075 Lovelace (1 ADA = 1000000 Lovelace), a postavljena je cijena od 6000000 Lovelace, tj. 6.00 ADA. Od tog iznosa 2.00 ADA bila naknada za izradu, 0.194 ADA je bila naknada za transakciju. Profit stvaratelja iznosio je 2.462 ADA te je prenesen na definiranu adresu za plaćanje. Višak od 3.538 ADA vraćen je kupcu. Razlika u odnosu na ostale korištene *blockchainove* je u tome što je potrebno uplatiti određeni zadani iznos na adresu za plaćanje, kada je pokrenuta prodaja, kako bi bila pokrenuta izrada nezamjenjivog *tokena*.

Na Near *blockchainu* plaćene su naknade za 4 transakcije. Kada je *near-cli* sučelju omogućeno korištenje Testnet korisničkog računa, tj. sučelje je dobilo javni ključ računa, plaćena je naknada od 0.00004 NEAR, a za izvršenje transakcije bilo je potrebno 419 Ggas („giga gas“) jedinica računalnih resursa [111], što je 0.419 Tgas. Naknada za *deploy* pametnog ugovora bila je 0.00223 NEAR, a izvršenje transakcije zahtijevalo je 22 Tgas („tera gas“) jedinica računalnih resursa [112]. Za inicijalizaciju pametnog ugovora iskorišteno je 7 Tgas jedinica računalnih resursa, a plaćena je naknada od 0.00074 NEAR [113]. Posljednja transakcija je bila ona za izradu nezamjenjivog *tokena* koja je za izvršenje trebala 7 Tgas jedinica računalnih resursa te naknadu u iznosu 0.0007 NEAR [114]. Svaka od njih će dodatno povećati naknadu koju će korisnik plaćati za čuvanje svih transakcija u memoriji.

Na Elgafar *blockchainu* cijena izrade kolekcije i pametnog ugovora iznosila je 1000 STARS, dok ostalih naknada nije bilo. Za tu transakciju potrošeno je 385 996 jedinica računalnih resursa [108]. Pošto je nezamjenjivi *token* izradio vlasnik ugovora, za izradu nije plaćena nikakva naknada [87]. U suprotnom bi kupac platio cijenu specificiranu u konfiguraciji. Izrada je zahtijevala 215 064 jedinica računalnih resursa [115].

7. PROCJENA TROŠKOVA

U trenutku pisanja, procjena naknade za izradu nezamjenjivog *tokena* na Ethereum *blockchainu* iznosila je 0.003 ETH [116], što odgovara ukupnoj naknadi koju je bilo potrebno platiti za izradu na Goerli *blockchainu*.

Istraživanjem postojećih transakcija na Stargaze Mainnet *blockchainu* utvrđeno je da su na njemu isti troškovi izrade kolekcije i pametnog ugovora kao što su bili prilikom testiranja na Elgafar *blockchainu* ili Stargaze Testnet *blockchainu*. Također, za izradu nezamjenjivog *tokena* vrijede ista pravila koja vrijede na Elgafar *blockchainu*.

Iste operacije na Near *blockchainu* uvijek će zahtijevati istu količinu računalnih resursa za obradu. Stoga, može se reći da će operacije izvršene prilikom testiranja na Testnetu zahtijevati istu količinu računalnih resursa i na Mainnetu. Cijena jedne jedinice računalnih resursa ovisi o trenutnom opterećenju mreže te zbog toga neće uvijek biti ista [117]. U trenutku pisanja cijena jedna jedinice je bila 0.0001 NEAR/Tgas [118]. Ukupna količina resursa za sve potrebne transakcije na Testnet iznosila je 36.419 Tgas te će ista količina biti potrebna i za transakcije na Mainnet. Prema trenutnoj cijeni jedne jedinice računalnih resursa, ukupna naknada će iznositi 0.0036419 NEAR.

Naknada za izradu nezamjenjivog *tokena* na Algorand *blockchainu* iznosi 0.001 Algo [119], što je viđeno i u detaljima nekoliko transakcija koje su izrađivale nezamjenjivi *token*.

Kao primjer izrade nezamjenjivih *tokena* na Cardano Mainnet *blockchainu* može se navesti izrada kolekcije digitalnih studentskih bedževa za Riteh Blockchain Team, točnije 20 bedževa za sve članove Teama i pet bedževa za voditelje projekata. Za izradu je plaćena naknada u iznosu od 0.386073 ADA [120].

8. DISKUSIJA

Prvotni plan testiranja izrade nezamjenjivog *tokena* na Cardano *blockchainu* bio je koristiti upute iz službene dokumentacije, ali već sama priprema sustava za izradu nije bila uspješna. Naime, izrada zahtjeva postojanje potpunog Cardano čvora na računalu. To znači da je prije izrade bilo potrebno sinkronizirati čvor sa cijelim *blockchainom*, tj. preuzeti sve postojeće blokove sa Testnet Cardano *blockchaina*. Međutim, sinkronizacija nije bila uspješna. Sinkronizacija je testirana sa nekoliko verzija komponente *cardano-node*, pri čemu su sve te verzije testirane i na Linux i na Windows operacijskim sustavima. Proces bi svaki put došao do otprilike 95 % i tada su se počele pojavljivati greške za koje istraživanjem nije pronađeno rješenje. Bilo je slučajeva kada je operacijski sustav Linux Ubuntu zaustavio *cardano-node* proces te je iz tog razlog testirano ograničavanje veličine stoga i broja korištenih jezgri procesora, no nije pomoglo.

Nakon izrade nezamjenjivog *tokena* pomoću Tangocrypto API-ja transakcije nisu bile vidljive u Cardanoscan Exploreru. Testirana je izrada pri kojoj se na adresu za plaćanje uplaćuju sredstva koristeći Typhon Wallet, čije su transakcije vidljive u Exploreru, ali u tom slučaju do izrade nije došlo. Sredstva su uplaćena na adresu za plaćanje, ali se nije pokrenula izrada, kao što je slučaj koristeći Nami Wallet.

9. ZAKLJUČAK

Cilj ovog rada je bio analizirati i testirati izradu nezamjenjivih *tokena* na Ethereum, Algorand, Cardano, Near i Cosmos *blockchainovima*. Tijekom izrade praćene su upute iz dokumentacije. Pažljivim praćenjem uputa svatko može izraditi nezamjenjivi *token*. Što se tiče nekakve kompleksnosti procesa, moglo bi se reći da je po tom pitanju izrada na Ethereum blockchainu najgora. Daleko od toga da se radi o kompleksnom procesu, ali vrijedi napomenuti. Ako se gleda broj transakcija koje je potrebno poslati na *blockchain*, najbolji je Algorand jer je jednom transakcijom nezamjenjivi *token* izrađen. Na ostalim *blockchainovima* potrebno je više transakcija, a svaka transakcija nosi sa sobom određenu naknadu.

Iako Testnet *tokeni* u kojima su plaćene naknade nemaju vrijednosti, može se napraviti usporedba prema njihovoj trenutnoj vrijednosti na Mainnetu. Uzevši to u obzir, najveća naknada plaćena je za izradu nezamjenjivog *tokena* na Stargaze Testnet *blockchainu* u sklopu Cosmos *blockchain* mreže. Zatim redom slijede Ethereuem, Cardano, Near i Algorand. Naknade na Algorand i Near *blockchainovima* su gotovo zanemarive, dok na Stargaze *blockchainu* iznosi čak oko 250 HRK. Na Ethereum blockchainu bi naknada iznosila oko 45 HRK, što je više od 5 puta manje u odnosu na Cosmos, a gotovo 4 puta više u odnosu na Cardano

Za niti jedan od *blockchainova* na kojima je testirana izrada nezamjenjivih *tokena* ne može se reći da je loš za tu svrhu. Algorand je najbolji s obzirom na jednostavnost procesa izrade i naknade za izradu, ali ostali testirani *blockchainovi* nisu daleko od njega. Niti jedan od njih se ne može otpisati i reći da se na njemu ne bi trebali izrađivati nezamjenjivi *tokeni*.

10.LITERATURA

[1] ICAEW: „History of blockchain“, s Interneta, https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-articles/what-is-blockchain/history, 11. rujna 2022.

[2] Seibold, S.; Samman, G.: „Consensus Immutable agreementfor the Internet of value“, KPMG LLP, Delaware, 2016.

[3] Dhongade, R.: „Blockchain technology basics“, s Interneta, https://www.spheregen.com/blockchain-technology-basics/, 25. lipnja 2022.

[4] Acharya D. P.: „An In-Depth Guide on the Types of Blockchain Nodes“, s Interneta, https://geekflare.com/finance/blockchain-nodes-guide/, 25. lipnja, 2022.

[5] Bitstamp: „ What are blockchain nodes?“, s Interneta, https://blog.bitstamp.net/post/what-are-blockchain-nodes/, 25.lipnja 2022.

[6] Abrol A.: „What are Blockchain nodes? Detailed Guide“, s Interneta, https://www.blockchain-council.org/blockchain/blockchain-nodes/, 26. lipnja 2022.

[7] Ethereuem: „The Ethereum Blockchain Explorer“, s Interneta, https://etherscan.io/, 26. lipnja 2022.

[8] Nibley, B.: „What is a crypto wallet? Understanding the software that allows you to store and transfer crypto securely“, s Interneta, https://www.businessinsider.com/personal-finance/crypto-wallet, 26. lipnja 2022.

[9] Frankenfield, J.: „Cryptocurrency Wallet“, s Interneta, https://www.investopedia.com/terms/b/bitcoin-wallet.asp, 26. lipnja 2022.

[10] Cointelegraph: „Fungible vs nonfungible tokens: What is the difference?“, s Interneta, https://cointelegraph.com/nonfungible-tokens-for-beginners/fungible-vs-nonfungible-tokens-what-is-the-difference, 26.lipnja 2022.

[11] Coinstouse: „What is NFT? How NFTs Work and Should You Invest in Them?“, s Interneta, https://coinstouse.com/2021/10/11/what-is-nft-how-nfts-work-should-you-invest-in-them/, 27. lipnja 2022.

[12] Wegrzyn K. E., Wang E.: „Types of Blockchain: Public, Private, or Something in Between“, s Interneta, https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between, 27. lipnja 2022.

[13] Simplilearn: „What is NFT and How Does NFT Work? The Ultimate Guide“, s Interneta, https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-nft, 27. lipnja 2022.

[14] Ethereuem: „Non-fungible tokens (NFT)“, s Interneta, https://ethereum.org/en/nft/#build-with-nfts, 27. lipnja 2022.

[15] Kramer A. S.: „Introduction To NFTS“, s Interneta, https://www.natlawreview.com/article/introduction-to-nfts, 27. lipnja 2022.

[16] Thune K.: „What Are NFT Royalties & How Do They Work?“, s Interneta, https://seekingalpha.com/article/4483346-nft-royalties, 27.lipnja 2022.

[17] LeewayHertz: „FRACTIONAL NFTS“, s Interneta, https://www.leewayhertz.com/fractional-nft/, 27. lipnja 2022.

[18] Hong A.: „Dissecting the Fractional protocol“, s Interneta, https://medium.com/coinmonks/dissecting-the-fractional-protocol-dc3867584bdb, 27 lipnja 2022.

[19] IBM: „What are smart contracts on blockchain?“, s Interneta, https://www.ibm.com/topics/smart-contracts, 27. lipnja 2022.

[20] Frankenfield, J: „Smart Contracts“, s Interneta, https://www.investopedia.com/terms/s/smart-contracts.asp, 27. lipnja 2022.

[21] Petersson D.: „How Smart Contracts Started And Where They Are Heading“, s Interneta, https://www.forbes.com/sites/davidpetersson/2018/10/24/how-smart-contracts-started-and-where-they-are-heading/, 20. kolovoza 2022.

[22] Coinbase: „What is a smart contract?“, s Interneta, https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract, 27. lipnja 2022.

[23] Levi S. D., Lipton A. B., Skadden, Arps, Slate, Meagher & Flom LLP: „An Introduction to Smart Contracts and Their Potential and Inherent Limitations“, s Interneta, https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/, 27. lipnja 2022.

[24] Lawton G.: „smart contract“, s Interneta, https://www.techtarget.com/searchcio/definition/smart-contract, 27. lipnja 2022.

[25] Simply Explained: „Smart contracts - Simply Explained“, s Interneta, https://www.youtube.com/watch?v=ZE2HxTmxfrI, 28. lipnja 2022.

[26] Makarov A.: „Top 6 smart contract platforms: a deep dive“, s Interneta, https://www.itransition.com/blog/smart-contract-platforms, 28. lipnja 2022.

[27] Sunday E.: „Top 5 smart contract programming languages for blockchain“, s Interneta, https://blog.logrocket.com/smart-contract-programming-languages/, 28. lipnja 2022.

[28] IPFS: „What is IPFS?“, s Interneta, https://docs.ipfs.tech/concepts/what-is-ipfs/#decentralization, 16. srpnja 2022.

[29] IPFS: „ IPFS powers the Distributed Web“, s Interneta, https://ipfs.io/, 16. srpnja 2022.

[30] IPFS: „How IPFS works“, s Interneta, https://docs.ipfs.tech/concepts/how-ipfs-works/#content-addressing, 16. srpnja 2022.

[31] Techtipsnreview: „What is IPFS? The Potential of IPFS in Blockchain“, s Interneta, https://techtipsnreview.com/what-is-ipfs-the-potential-of-ipfs-in-blockchain/, 16. srpnja 2022.

[32] IPFS: „IPFS Gateway“, s Interneta, https://docs.ipfs.tech/concepts/ipfs-gateway/, 17. srpnja 2022.

[33] Ethereum: „The foundation for our digital future“, s Interneta, https://ethereum.org/en/what-is-ethereum/, 17. srpnja 2022.

[34] Castor A.: „Why Ethereum is switching to proof of stake and how it will work“, s Interneta, https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/, 17. srpnja 2022.

[35] Ethereum: „Private Ethereum for enterprise“, s Interneta, https://ethereum.org/en/enterprise/private-ethereum/, 17. srpnja 2022.

[36] Ethereum: „PROOF-OF-WORK (POW)“, s Interneta, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/, 17. srpnja 2022.

[37] Ledger Academy: „What is Proof-of-Work“, s Interneta, https://www.ledger.com/academy/blockchain/what-is-proof-of-work, 1. kolovoza 2022.

[38] Ethereum: „Ethereum-powered tools and services“, s Interneta, https://ethereum.org/en/dapps/, 17. srpnja 2022.

[39] Ethereuem: „GAS AND FEES“, s Interneta, https://ethereum.org/en/developers/docs/gas/, 17. srpnja 2022.

[40] Tarcan H.: „ERC-721 NON-FUNGIBLE TOKEN STANDARD“, s Interneta, https://ethereum.org/en/developers/docs/standards/tokens/erc-721/, 5. kolovoza 2022.

[41] OpenSea: „Metadata Standards“, s Interneta, https://docs.opensea.io/docs/metadata-standards, 5. kolovoza 2022.

[42] Ethereuem: „PROOF-OF-STAKE (POS)“, s Interneta, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/, 17. srpnja 2022.

[43] Millman R., Graves S., Kelly L. J.: „What Is Ethereum 2.0? Ethereum's Consensus Layer and Merge Explained“, s Interneta, https://decrypt.co/resources/what-is-ethereum-2-0, 1. kolovoza 2022.

[44] Algorand: „Algorand’s Commitment to Sustainable Blockchain“, s Interneta, https://www.algorand.com/about/sustainability, 18. srpnja 2022.

[45] Algorand: „Why Algorand?“, s Interneta, https://developer.algorand.org/docs/get-started/basics/why_algorand/, 18. srpnja 2022.

[46] Algorand: „TECHNOLOGY“, s Interneta, https://www.algorand.com/technology/algorand-protocol, 18. srpnja 2022.

[47] Algorand: „ALGORAND PROTOCOL OVERVIEW“, s Interneta, https://www.algorand.com/technology/protocol-overview, 27. srpnja 2022.

[48] Avila Visintin T. D.: „Pure Proof of Stake (PPoS) | Consensus in Algorand explained“, s Interneta, https://cryptowebacademy.com/pure-proof-of-stake-ppos-consensus-in-algorand-explained/, 1. kolovoza 2022.

[49] Algorand: „ALGORAND FEATURES & CAPABILITIES IN LAYER-1“, s Interneta, https://www.algorand.com/technology, 18. srpnja 2022.

[50] Algorand: „Create an NFT“, s Interneta, https://developer.algorand.org/docs/get-started/tokenization/nft/, 19. srpnja 2022.

[51] Algorand: „Algorand Standard Assets (ASAs)“, s Interneta, https://developer.algorand.org/docs/get-details/asa/, 19. srpnja 2022.

[52] Algorand: „Structure“, s Interneta, https://developer.algorand.org/docs/get-details/transactions/, 19.srpnja 2022.

[53] Algorand: „Atomic transfers“, s Interneta, https://developer.algorand.org/docs/get-details/atomic_transfers/, 19. srpnja 2022.

[54] Cardano: „Documentation for the Cardano ecosystem“, s Interneta, https://docs.cardano.org/, 27. srpnja 2022.

[55] Cryptopolitan: „Speed and Scalability: Comparing Ethereum, Solana, Avalanche, Cardano, and the Internet Computer“, s Interneta, https://www.cryptopolitan.com/speed-and-scalability-comparing-ethereum-solana-avalanche-cardano-and-the-internet-computer/, 31. srpnja 2022.

[56] Cardano: „Cardano fee structure“, s Interneta, https://docs.cardano.org/explore-cardano/fee-structure, 27. srpnja 2022.

[57] Cardano: „Consensus explained“, s Interneta, https://docs.cardano.org/learn/consensus-explained, 27. srpnja 2022.

[58] Cardano: „Stake pools“, s Interneta, https://docs.cardano.org/core-concepts/stake-pools, 28. srpnja 2022.

[59] Cardano: „Ouroboros“, s Interneta, https://cardano.org/ouroboros/, 29. srpnja 2022.

[60] Kiayias, A.; Russell, A.; David, B.; Oliynykov, R.: „Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol“, 2019.

[61] Lopez de Lara C.: „How Ouroboros Proof of stake works?“, s Interneta, https://medium.com/@carloslopezdelara/whats-ouroboros-the-cardano-proof-of-stake-protocol-ad4b958e152e, 2. kolovoza 2022.

[62] Cardano: „Minting NFTs“, s Interneta, https://developers.cardano.org/docs/native-tokens/minting-nfts, 30. srpnja 2022.

[63] Lovelace Academy: „NFT Minting Guide“, s Interneta, https://learn.lovelace.academy/tokens/nft-minting-guide/, 30. srpnja 2022.

[64] Cardano: „Minting Native Assets“, s Interneta, https://developers.cardano.org/docs/native-tokens/minting/, 30. srpnja 2022.

[65] Cardano Ledger: „Minting policies and the multiasset ledger“, s Interneta, https://cardano-ledger.readthedocs.io/en/latest/explanations/policies.html, 31. srpnja 2022.

[66] Parrino D.: „What is NEAR?“, s Interneta, https://docs.near.org/concepts/what-is-near, 31. srpnja 2022.

[67] Near: „Economics in a Sharded Blockchain“, s Interneta, https://near.org/papers/economics-in-sharded-blockchain/, 31. srpnja 2022

[68] Near: „ETH <> NEAR Rainbow Bridge“, s Interneta, https://near.org/bridge/, 31. srpnja 2022.

[69] Near: „The NEAR White Paper“, s Interneta, https://near.org/papers/the-official-near-white-paper/, 31. srpnja 2022.

[70] Polosukhin, I.: „Thresholded Proof Of Stake“, s Interneta, https://near.org/blog/thresholded-proof-of-stake/, 31. srpnja 2022.

[71] Singhania A.: „Consensus“, s Interneta, https://nomicon.io/ChainSpec/Consensus, 7. kolovoza 2022.

[72] Parrino D.: „Transactions in the Blockchain Layer“, s Interneta, https://nomicon.io/ChainSpec/Transactions, 11. rujna 2022.

[73] Skidanov A.; Polosukhin, I.: „Nightshade: Near Protocol Sharding Design“, s Interneta, https://near.org/downloads/Nightshade.pdf, 8. kolovoza 2022.

[74] Near team: „NEAR Launches Nightshade Sharding, Paving the Way for Mass Adoption“, s Interneta, https://near.org/blog/near-launches-nightshade-sharding-paving-the-way-for-mass-adoption/, 8. kolovoza 2022.

[75] Near: „NEAR REST API SERVER“, s Interneta, https://github.com/near-examples/near-api-rest-server, 31. srpnja 2022.

[76] Parrino D.: „Non Fungible Tokens“, s Interneta, https://docs.near.org/develop/relevant-contracts/nft, 1. kolovoza 2022.

[77] Ori-near: „Metadata“, s Interneta, https://nomicon.io/Standards/Tokens/NonFungibleToken/Metadata, 1. kolovoza 2022.

[78] Cosmos: „Welcome to Cosmos“, s Interneta, https://cosmos.network/intro, 3. kolovoza 2022.

[79] Cosmos: „What is Cosmos?“, s Interneta, https://v1.cosmos.network/intro, 3. kolovoza 2022.

[80] Cosmos: „Introduction“, s Interneta, https://hub.cosmos.network/main/hub-overview/overview.html, 3. kolovoza 2022.

[81] Cosmos: „High-level Overview“, s Interneta, https://docs.cosmos.network/v0.46/intro/overview.html, 3. kolovoza 2022.

[82] IBC: „INTER-BLOCKCHAINCOMMUNICATION PROTOCOL“, s Interneta, https://ibcprotocol.org/, 3. kolovoza 2022.

[83] Cosmos: „The Internet of Blockchains.“, s Interneta, https://cosmos.network/, 4. kolovoza 2022.

[84] Cosmos: „Cosmos Whitepaper“, s Interneta, https://v1.cosmos.network/resources/whitepaper#, 3. kolovoza 2022.

[85] Tedermint: „What is Tendermint“, s Interneta, https://docs.tendermint.com/v0.34/introduction/what-is-tendermint.html, 5. kolovoza 2022.

[86] Cosmos: „ADR 43: NFT Module“, s Interneta, https://docs.cosmos.network/master/architecture/adr-043-nft-module.html#further-discussions, 4. kolovoza 2022.

[87] Stargaze: „Launching an NFT project“, s Interneta, https://docs.stargaze.zone/guides/readme, 4. kolovoza 2022.

[88] Ethereum: „HOW TO WRITE & DEPLOY AN NFT (PART 1/3 OF NFT TUTORIAL SERIES)“, s Interneta, https://ethereum.org/en/developers/tutorials/how-to-write-and-deploy-an-nft/, 12. kolovoza 2022.

[89] Ethereum: „HOW TO MINT AN NFT (PART 2/3 OF NFT TUTORIAL SERIES)“, s Interneta, https://ethereum.org/en/developers/tutorials/how-to-mint-an-nft/, 12. kolovoza 2022.

[90] Ethereuem: „HOW TO VIEW YOUR NFT IN YOUR WALLET (PART 3/3 OF NFT TUTORIAL SERIES)“, s Interneta, https://ethereum.org/en/developers/tutorials/how-to-view-nft-in-metamask/, 12. kolovoza 2022.

[91] Etherscan: „Transaction Details“, s Interneta, https://goerli.etherscan.io/tx/0x1a571c473d8dd96975f34b323022a951f30ada8138b868e2708ad1e6031de00a, 23. kolovoza 2022.

[92] Algorand: „CreateNFTJavaScript“, s Interneta, https://replit.com/@Algorand/CreateNFTJavaScript, 15. kolovoza 2022.

[93] Algorand: „Algorand Testnet Dispenser“, s Interneta, https://dispenser.testnet.aws.algodev.network/, 16. kolovoza 2022.

[94] Algorand Blockchain Explorer: „Transaction Details“, s Interneta, https://testnet.algoexplorer.io/tx/SQNEGX3PXPMWZMPZAAZ6PZUMH76A3WGVOMJ4ZSXAFOG27LW2WNTA, 2. rujna 2022.

[95] Algorand Blockchain Explorer, „Asset Overview“, s Interneta, https://testnet.algoexplorer.io/asset/107757783, 2. rujna 2022.

[96] Tangocrypto API: „Create NFT collection“, s Interneta, https://www.tangocrypto.com/api-reference/#/operations/nft-collection, 26. kolovoza 2022.

[97] Tangocrypto API: „Create NFT“, s Interneta, https://www.tangocrypto.com/api-reference/#/operations/nft-create-nft, 26. kolovoza 2022.

[98] Tangocrypto API: „Create NFT sale“, s Interneta, https://www.tangocrypto.com/api-reference/#/operations/create-nft-sale, 26. kolovoza 2022.

[99] Near: „Minting NFTs“, s Interneta, https://docs.near.org/tutorials/nfts/minting-nfts, 18. lipnja 2022.

[100] Near Testnet Explorer: „Transaction“, s Interneta, https://explorer.testnet.near.org/transactions/7njS6biZHiKW4sY1dKQCdqqw3D4fPzS4xyzfNms9rKaQ, 2. rujna 2022.

[101] Stargaze: „Launching an NFT project“, s Interneta, https://docs.stargaze.zone/guides/readme, 22. kolovoza 2022.

[102] Stargaze: „1. Setup a basic project“, s Interneta, https://docs.stargaze.zone/guides/readme/1.-setup-a-basic-project, 22. kolovoza 2022.

[103] Stargaze: „3. Add assets and metadata“, s Interneta, https://docs.stargaze.zone/guides/readme/3.-add-assets-and-metadata, 22. kolovoza 2022.

[104] Stargaze: „NFT.storage (script)“, s Interneta, https://docs.stargaze.zone/guides/readme/3.-add-assets-and-metadata/3.-add-assets-and-metadata, 22. kolovoza 2022.

[105] Stargaze: „2. Configure your project“, s Interneta, https://docs.stargaze.zone/guides/readme/2.-configure-your-project, 22. kolovoza 2022.

[106] Stargaze: „4. Instantiate minter contract on testnet“, s Interneta, https://docs.stargaze.zone/guides/readme/4.-instantiate-minter-contract-on-testnet, 22. kolovoza 2022.

[107] Stargaze: „6. Mint from your contract“, s Interneta, https://docs.stargaze.zone/guides/readme/6.-mint-from-your-contract, 22. kolovoza 2022.

[108] Ping Explorer: „Transaction“, s Interneta, https://testnet-explorer.publicawesome.dev/stargaze/tx/B282A27CFC58F7EC894ABF57CC36CD67B560A56E12ACF0ED5A1AC43F5421B95A, 2. rujna 2022.

[109] Stargaze: „RitehNFT“, s Interneta, https://testnet.publicawesome.dev/media/stars1lt6qyqckmlctgmr462h7fssdtde3qn2sw3sw0p3e2k8ejp6al8msluzv5r/1, 2. rujna 2022.

[110] Etherscan: „Transaction Details“, s Interneta, https://goerli.etherscan.io/tx/0x98159759117de3f3aa35524411c55e47f7e1bcc5bfffb2800e89a5c5cf93c5ce, 23. kolovoza 2022.

[111] Near Testnet Explorer: „Transaction“, s Interneta, https://explorer.testnet.near.org/transactions/EdYnEm8REZQHWq1W6FZx7gDPPhLd5QsKF9SZHM5YzWh4, 2. rujna 2022.

[112] Near Testnet Explorer: „Transaction“, s Interneta, https://explorer.testnet.near.org/transactions/DVpgjEAJkLpDTWToGnjZUgvuaByctAVz1iyRoEKJWee, 2. rujna 2022.

[113] Near Testnet Explorer: „Transaction“, s Interneta, https://explorer.testnet.near.org/transactions/FrLocZ4VhZvESBauxD3n2wWG7FGQWNUc6BzwG2CFu3Uc, 2. rujna 2022.

[114] Near Testnet Explorer: „Transaction“, s Interneta, https://explorer.testnet.near.org/transactions/7njS6biZHiKW4sY1dKQCdqqw3D4fPzS4xyzfNms9rKaQ, 2. rujna 2022.

[115] Ping Explorer: „Transaction“, s Interneta, https://testnet-explorer.publicawesome.dev/stargaze/tx/9BD695AB66140DB246FB7446E8804D2A9FBEBB71CE0588B1CB46698AFD0002E0, 2. rujna 2022.

[116] Gas Calculator: „Rarible“, s Interneta, https://www.gwei.at/, 5. rujna 2022.

[117] Near: „Gas“, s Interneta, https://docs.near.org/concepts/basics/transactions/gas, 8. rujna 2022.

[118] Near: „Explore the NEAR Blockchain.“, s Interneta, https://explorer.near.org/, 15. rujna 2022.

[119] Algorand: „Calling All Creators...“, s Interneta, https://www.algorand.foundation/nfts, 6. rujna 2022.

[120] Cardanoscan: „Transaction Details“, s Interneta, https://cardanoscan.io/transaction/2804b092539af64ada028965e2ab3e2c5c37615767d330540b1b9cb83282a93e?fbclid=IwAR3AekwYDhzPhayaGsUY5jJQHBma3unS4TWPqWKVgZ0U_so-5-BxRf0egl8, 13. rujna 2022.

SAŽETAK

U ovom radu zadatak je bio analizirati i testirati izradu nezamjenjivog *tokena* (NFT) na Ethereum, Algorand, Cardano, Near i Cosmos *blockchainovima*. Prvi dio rada sadrži detaljan opis *blockchain* tehnologije i *blockchain* tehnologija korištenih u radu. Zatim slijedi opis *blockchainova* na kojima će biti testirana izrada nezamjenjivih *tokena*. Potom je testirana izrada na spomenutim *blockchainovima*. Nakon provođenja testiranja rezultati su analizirani. Na kraju rada nalazi se zaključak.

Ključne riječi: **NFT, *blockchain*, Ethereum, Algorand, Cardano, Near, Cosmos**

ABSTRACT

In this paper task was to analyze and test minting non-fungible tokens (NFT) on Ethereum, Algorand, Cardano, Near i Cosmos *blockchains*. First part contains detailed description of blockchain technology and blockchain technologies used in this paper. It was followed by description of blockchains on which minting of NFTs is going to be tested. After that, minting was tested on mentioned blockchains. When tests were completed, results were analyzed. At the end there is conclusion.

Key words: **NFT, *blockchain*, Ethereum, Algorand, Cardano, Near, Cosmos**