

# Primjena Blockchain tehnologije u 5G sustavima

---

**Ećimović, Mihael**

**Undergraduate thesis / Završni rad**

**2023**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:200:461246>

*Rights / Prava:* [In copyright](#) / [Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2024-07-16**

*Repository / Repozitorij:*

[Faculty of Electrical Engineering, Computer Science and Information Technology Osijek](#)



**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU  
ELEKTROTEHNIČKI FAKULTET**

**Preddiplomski sveučilišni studij računarstva**

**PRIMJENE TEHNOLOGIJE POVEZANIH BLOKOVA  
U 5G SUSTAVIMA**

**Završni rad**

**Mihael Ećimović**

**Osijek, 2023.**

**FERIT**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA  
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK****Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju**

Osijek, 15.09.2023.

Odboru za završne i diplomske ispite

**Prijedlog ocjene završnog rada na  
preddiplomskom sveučilišnom studiju**

|   |  |
|---|--|
| <b>Ime i prezime Pristupnika:</b>   | Mihael Ećimović  |
| <b>Studij, smjer:</b>   | Programsko inženjerstvo  |
| <b>Mat. br. Pristupnika, godina upisa:</b>  | R4487, 27.07.2020.   |
| <b>OIB Pristupnika:</b>   | 61106267996  |
| <b>Mentor:</b>  | prof. dr. sc. Marijan Herceg   |
| <b>Sumentor:</b>  | ,  |
| <b>Sumentor iz tvrtke:</b>  |  |
| <b>Naslov završnog rada:</b>  | Primjena Blockchain tehnologije u 5G sustavima   |
| <b>Znanstvena grana rada:</b>   | <b>Telekomunikacije i informatika (zn. polje elektrotehnika)</b>   |
| <b>Zadatak završnog rad:</b>  | U sklopu završnog rada potrebno je proučiti područja primjene Blockchain tehnologije u sustavima zasnovanim na 5G mrežama. Nadalje, potrebno je napraviti komparativnu analizu prednosti i nedostataka primjene Blockchain-a u usporedbi s drugim tehnologijama. |
| <b>Prijedlog ocjene završnog rada:</b>  | Dobar (3)  |
| <b>Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:</b> | Primjena znanja stečenih na fakultetu: 1 bod/boda<br>Postignuti rezultati u odnosu na složenost zadatka: 1 bod/boda<br>Jasnoća pismenog izražavanja: 1 bod/boda<br>Razina samostalnosti: 2 razina  |
| <b>Datum prijedloga ocjene od strane mentora:</b>   | 15.09.2023.  |
| <b>Datum potvrde ocjene od strane Odbora:</b>   | 24.09.2023.  |
| Potvrda mentora o predaji konačne verzije rada:   | <i>Mentor elektronički potpisao predaju konačne verzije.</i>   |
|   | Datum:   |

**FERIT**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA  
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK****IZJAVA O ORIGINALNOSTI RADA**

Osijek, 25.09.2023.

|                                  |                         |
|----------------------------------|-------------------------|
| Ime i prezime studenta:          | Mihael Ećimović         |
| Studij:                          | Programsko inženjerstvo |
| Mat. br. studenta, godina upisa: | R4487, 27.07.2020.      |
| Turnitin podudaranje [%]:        | 1                       |

Ovom izjavom izjavljujem da je rad pod nazivom: **Primjena Blockchain tehnologije u 5G sustavima**

izrađen pod vodstvom mentora prof. dr. sc. Marijan Herceg

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija. Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

# SADRŽAJ

|   |           |
|---|-----------|
| <b>1. UVOD .....</b>  | <b>1</b>  |
| <b>2. OPIS TEHNOLOGIJE POVEZANIH BLOKOVA I 5G MREŽA .....</b>           | <b>3</b>  |
| 2.1 TEHNOLOGIJA POVEZANIH BLOKOVA.....                                  | 3         |
| 2.2 5G SUSTAV .....   | 6         |
| <b>3. PRIMJENA BLOCKCHAIN TEHNOLOGIJE U 5G SUSTAVIMA .....</b>          | <b>8</b>  |
| 3.1. BLOCKCHAIN ZA RAČUNARSTVO U OBLAKU .....                           | 8         |
| 3.2. BLOCKCHAIN ZA 5G DIJELJENJE INFRASTRUKTURE .....                   | 10        |
| 3.3. PRIMJENA BLOCKCHAINA U MEĐUNARODNOM ROAMINGU .....                 | 12        |
| 3.4. PRIMJENA BLOCKCHAINA U SOFTVERSKI DEFINIRANOM UMREŽAVANJU .....    | 15        |
| 3.5. BLOCKCHAIN ZA MASOVNU PODRŠKU 5G INFRASTRUKTURE .....              | 17        |
| 3.6. PRIMJENA BLOCKCHAINA U SEGMENTACIJI MREŽE .....                    | 18        |
| 3.7. PRIMJENA BLOCKCHAIN TEHNOLOGIJE U 5G SIGURNOSNIM USLUGAMA .....    | 20        |
| <b>4. PREDNOSTI I NEDOSTACI PRIMJENE BLOCKCHAINA U 5G MREŽAMA .....</b> | <b>22</b> |
| 4.1. PREDNOSTI BLOCKCHAINA U 5G MREŽAMA .....                           | 22        |
| 4.2. NEDOSTACI BLOCKCHAINA U 5G MREŽAMA .....                           | 24        |
| <b>5. ZAKLJUČAK .....</b>   | <b>27</b> |
| <b>LITERATURA .....</b>   | <b>28</b> |
| SAŽETAK .....   | 31        |
| ABSTRACT.....   | 32        |
| ŽIVOTOPIS .....   | 33        |

## 1. UVOD

Peta generacija tehnologije, poznata kao 5G, predstavlja sljedeću važnu fazu globalne evolucije telekomunikacija te se postavlja diljem cijeloga svijeta. To je novi svjetski bežični standard poslije 1G, 2G, 3G, i 4G mreža. 5G omogućava novu vrstu mreže koja je dizajnirana da poveže sve i svakoga, uključujući strojeve, objekte i uređaje. Cilj 5G-a je pružanje više gigabita po sekundi za prijenos podataka, izuzetno nisku latenciju, veću pouzdanost, ogroman kapacitet mreže, povećanu dostupnost te jednako korisničko iskustvo velikom broju korisnika. Veća učinkovitost i poboljšana efikasnost doprinose boljim korisničkim doživljajima i povezuju nove industrije [1]. 5G mobilne mreže omogućavaju revoluciju globalnih industrija i pružanje odmah vidljivih utjecaja na korisnike i sudionike poslovanja. Kako bi se ovi ciljevi mogli postići, 5G će raditi na visokim frekvencijama, tako zvanim milimetarskim valovima koji rade na frekvencijama preko 30 GHz-a. Posljedica toga su signali koji putuju manjim udaljenostima, što zahtjeva više mobilnih stanica koje bi pokrivale jednako 4G područje i rezultira većim troškovima u pravljenju infrastrukture. Kako bi se ti troškovi smanjili, nove opcije se razmatraju, npr. masovna podrška (engl. crowdsourcing), dijeljenje roaminga i dijeljenje spektra. Još jedan izazov je rješavanje upravljačkih i servisnih mogućnosti ogromnih komunikacija strojeva sa zahtjevom podrške od barem 1 milijun uređaja po kilometru kvadratnom. Jako veliki broj distribuiranih i heterogenih Internet stvari (engl. Internet of Things – IoT) uređaja predstavljaju nove izazove u vezi autentikacije i skalabilnosti 5G mreža [2]. U ovom radu opisana je mogućnost uporabe tehnologija povezanih blokova (engl. blockchain) koja može imati važnu ulogu u rješavanju problema decentralizacije, sigurnosti i troškova u 5G mrežama.

U 5G eri, nepromjenjivost, decentralizacija i transparentnost ključni su sigurnosni čimbenici koji osiguravaju uspješno implementiranje novih usluga poput prikupljanja podataka *IoT*-a, autonomnih vozila, bespilotnih letjelica itd. Među postojećim tehnologijama, *blockchain* je jedna od najboljih za ispunjavanje takvih sigurnosnih zahtjeva. *Blockchain* je tehnologija distribuirane knjige koja je prvi put korištena kao javna digitalna knjiga kriptovalute *Bitcoin*. *Blockchain* je decentralizirana, nepromjenjiva i transparentna baza podataka. Koncept *blockchaina* temelji se na arhitekturi mreže vršnih čvorova u kojoj se svi sudionici u mreži upravljaju informacijama o transakcijama i informacije nisu pod kontrolom nijedne središnje vlasti. *Blockchain* ima nekoliko poželjnih svojstava koji se mogu primijeniti u 5G mrežama, a to su decentralizacija, nepromjenjivost, odgovornost i pouzdana pohrana podataka, što značajno poboljšava sigurnost mreže i smanjuje operativne troškove. Brzi razvoj i prihvaćanje *blockchaina* otvara put za sljedeću

generaciju financijskih i industrijskih usluga. Trenutno se istražuje i primjenjuje *blockchain* tehnologija u raznim područjima kao što su internet stvari, računarstvo na rubu, pametni gradovi, autonomna vozila, itd.

Od kombinacije *blockchaina* i 5G-a također se očekuje otvaranje puteva za nove mobilne usluge. 5G se odnosi na povezivanje različitih uređaja i složenih mreža koje će do 2030. godine međusobno povezati više od 500 milijardi mobilnih uređaja. Ultra-guste mreže malih ćelija omogućit će veze i energetska učinkovitost radijskih veza s visokim brzinama prijenosa podataka i niskim latencijama. Međutim, to uvodi pitanja povjerenja i sigurnosti među složenim podmrežama. Zato je vrlo važno osigurati pouzdanu suradnju među različitim uređajima u 5G mobilnim mrežama. Veliki izazov za trenutne platforme 5G-a je potreba za osiguravanjem otvorenog, transparentnog i sigurnog sustava među velikim brojem uređaja i korisnika. *Blockchain* s inovativnim konceptima decentraliziranosti može pružiti visoku razinu privatnosti podataka, sigurnosti, transparentnosti i nepromjenjivosti za pohranu različitih podataka 5G-a [3]. Stoga se 5G smatra važnim alatom čija se integracija sa *blockchainom* aktivno istražuje i implementira. Glavni fokus u ovom radu bio je na potencijal i prednosti primjene *blockchain* tehnologije u tehnologijama i dijelovima 5G sustava te je napravljena komparativna analiza prednosti i nedostataka koje ta primjena može donijeti.

## 2. OPIS TEHNOLOGIJE POVEZANIH BLOKOVA I 5G MREŽA

### 2.1 TEHNOLOGIJA POVEZANIH BLOKOVA

*Blockchain* možemo definirati kao tehnologiju distribuirane knjige koja bilježi transakcije u mreži koja je zasnovana na komunikaciji između jednakih (engl. peer-to-peer – P2P), gdje su sva računala povezana i imaju jednaka prava i odgovornosti, umjesto korištenja jednog ili više poslužitelja. Kod *blockchaina*, svi su zapisi spremljeni na mnogo međusobno povezanih sustava koji čuvaju jednake informacije. Ako ažuriranja nekog računala nisu autenticirana, mreža ih odbija. U *blockchainu*, brojne transakcije razmjene vrijednosti grupirane su u nekoliko blokova i svaki blok povezan je na prijašnji blok. Korištenjem mehanizama jamstva i kriptografskog povjerenja, svaki blok nepovratno bilježi zapise diljem *peer-to-peer* mreže. *Blockchain* tehnologija razlikuje se od tehnologije baze podataka. U *blockchainu*, novi unosi dodani su na kraj lanca i nitko ne smije brisati ili uređivati podatke dok kod baza podataka središnji administrator može izmjenjivati i brisati podatke.

*Blockchain* tehnologija uglavnom se temelji na kriptografiji, distribuiranom računarstvu i teoriji igara. Glavna knjiga nalazi se u svakom čvoru. Ako zlonamjerni korisnik pokuša hakirati profil i ukrasti novce ili informacije, mora hakirati puno čvorova i izmijeniti puno glavnih knjiga. Da bi *blockchain* mreža bila hakirana, više od 51% čvorova te mreže mora biti hakirano, što je vrlo teško. Može postojati više korisnika koji rade kao upravitelji sigurnosnih kopija te koji vrata informacije probijenih računa.

Merkle stabla, pametni ugovori, *hash* i konsenzus algoritmi su pojmovi bitni za razumijevanje *blockchaina* te daljnjeg povezivanja *blockchaina* i 5G sustava. *Hash* funkcija je funkcija koja pretvara podatke raznih duljina u podatke sa fiksnom duljinom. Ti novonastali podaci zovu se *hash* vrijednosti. Merkle stablo je struktura podataka koja se koristi za pohranjivanje *hash* vrijednosti svakog podatka u velikoj bazi podataka tako da verifikacija baze podataka može biti efikasna. Dakle, merkle stablo omogućuje korisnicima provjeru pripada li određena transakcija bloku. Pametni ugovor je računalni program koji podržava automatsko izvršavanje procesa transakcije ako su predefimirani uvjeti zadovoljeni. Konsenzus algoritam je proces postizanja sporazuma među korisnicima u *blockchain* mreži. Konsenzus je vrlo važan za očuvanje sigurnosti i integriteta *blockchaina* jer onemogućava napadačima da izmjenjuju glavnu knjigu. On je odgovoran za odlučivanje koje transakcije će biti dodane u lanac i osigurava da svi čvorovi u mreži imaju jednaku kopiju glavne knjige. Bez konsenzus algoritama, *blockchain* mreža bila bi osjetljiva na



prevare i napade jer se ne bi moglo osigurati da svaki čvor ima istu kopiju glavne knjige. Postoje razne vrste konsenzus algoritama, a najpoznatiji je dokaz o radu (engl. Proof of Work).

Dokaz o radu prvi je konsenzus algoritam koji se još uvijek koristi kod *Bitcoina* i mnogih drugih kriptovaluta. Kod njega, rudari rješavaju složene matematičke zadatke kako bi potvrdili transakcije i dodali nove blokove u *blockchain*. Prvi rudar koji uspije riješiti matematički problem nagrađen je novo iskovanim kovanicama. Dokaz o radu poznat je po svojoj sigurnosti, ali troši puno energije i transakcije se sporo procesiraju. Zbog toga se traže novi konsenzus algoritmi koji bi mogli nadomjestiti ove nedostatke, a najpopularniji je dokaz o udjelu (engl. Proof of Stake) čije se različitosti od dokaza o radu mogu vidjeti na slici 2.1. Dizajniran je da bude brži i energetski efikasniji, ali manje sigurniji. Kod njega, umjesto rudara koji moraju rješavati zadatke, biraju se validatori na temelju količine kriptovaluta koje drže te oni potvrđuju transakcije i dodavaju nove blokove u *blockchain* i nagrađeni su na temelju njihovog udjela [4].



Slika 2.1. Usporedba dokaza o radu i dokaza o udjelu [22]

Postoje 3 vrste *blockchaina*: javni *blockchain*, privatni *blockchain* i konzorcijski *blockchain*. U javnom *blockchainu* svi mogu prisustvovati u mreži u pisanju, čitanju i provjeri podataka. Otvoren je i transparentan za sve. Pošto nema nikakvih središnjih administratora, sve odluke se donose

prema raznim decentraliziranim algoritmima konsenzusa, kao što su dokaz o udjelu, dokaz o radu i mnogi drugi. Privatni *blockchain* privatna je imovina organizacije ili pojedinca. Za razliku od javnog *blockchaina*, postoji odgovorna osoba koja vodi brigu o svim ključnim aspektima mreže. U njemu se algoritam konsenzusa razvija uz sudjelovanje centralne odgovorne osobe, koja može dodijeliti pravo rudarenja bilo kome. Stoga je opet centraliziran jer su mnoga prava dodijeljena pojedincima. Privatni *blockchain* je kriptografski osiguran i ekonomičan. Konzorcijalni *blockchain* pokušava maknuti nedostatke privatnog *blockchaina* gdje jedan entitet ima sva prava. U konzorcijalnom *blockchainu* više entiteta imaju prava. Skup predstavnika, pojedinaca ili tvrtki udružuje se i donosi odluke za opću korist *blockchain* mreže. Konzorcijalni *blockchain* je brz i sigurniji je od javnog *blockchaina*. Primjeri konzorcijalnog *blockchaina* su *r3* i *EFW*.

Najpoznatija svojstva *blockchaina* su:

- Decentraliziranost - omogućuje uklanjanje središnjih autoriteta i posrednika, kao što su banke i to umanjuje troškove i rizik.
- Transparentnost - svi podaci su javni i ne mogu se lako mijenjati, a provjera tih podataka je vrlo teška.
- Redundantnost - svaki korisnik ima kopiju datoteke što otežava hakiranje te datoteke kada korisnik nije aktivan.
- Neizbrisivost - teško je mijenjati zapise, a algoritam konsenzusa razvijen je protokolom.

Prednosti *blockchaina* su:

- Sigurnost – sigurnost je jedan od glavnih problema današnjeg digitalnog svijeta. Kod *blockchaina*, sve potvrđene ili obavljene transakcije trajno su pohranjene u blokovima koje nitko ne može obrisati ni izmijeniti.
- Distribuiranost – podržava brojna računala koja se nalaze diljem svijeta. Na primjer, *Ethereum*, sustav baziran na *blockchainu*, podržava skoro sve korisnike da se pridruže njegovoj mreži jednostavnim instaliranjem softvera.
- Efikasnost – efikasnost mreže može biti poboljšana korištenjem *blockchaina* kada financijske strane međusobno surađuju. Korištenjem *blockchaina* može se razviti sustav koji poboljšava učinkovitost mreže u stvarnom vremenu.
- Transparentnost – podaci su objavljeni na zajedničkoj platformi, a zainteresirane strane i regulator mogu jednostavno dobiti uvid u tu platformu

- Povjerenje – većina korisnika mora se složiti sa podacima prije nego se dodaju u *blockchain* mrežu, što je drukčije nego u centraliziranoj mreži. Dakle, povjerenje je povećano za pisanje, mijenjanje i čitanje podataka. [5]

## 2.2 5G SUSTAV

Promet mobilnih i bežičnih mreža eksponencijalno se povećava. S brzim povećanjem broja povezanih uređaja, pojavljuju se određeni izazovi koji se mogu riješiti povećanjem kapaciteta i poboljšanjem energetske učinkovitosti, troškova i iskorištenosti frekvencijskog spektra te pružanjem bolje skalabilnosti za obradu rastućeg broja povezanih uređaja. Za viziju svijeta s potpunom komunikacijom u odnosu na današnje mreže, opći tehnički cilj je pružiti ideju sustava koja podržava:

- 1000 puta veći volumen podataka po površini.
- 10 do 100 puta veći broj povezanih uređaja.
- 10 do 100 puta veću tipičnu brzinu prijenosa podataka korisnika.
- 10 puta dulji vijek trajanja baterije za uređaje niske snage za masovnu komunikaciju strojeva.
- Smanjenje vremena kašnjenja od kraja do kraja (engl. end to end - E2E) za 5 puta.

Kako bi se ti ciljevi mogli ispuniti, 5G mreže moraju upotrijebiti razne tehnologije, kao što su računarstvo na oblaku (engl. cloud computing), računarstvo na rubu, softverski definirano umrežavanje, virtualizacija mrežnih funkcija, segmentiranje mreže, komunikacija uređaja do uređaja, milimetarska valnu komunikacija itd.

Računarstvo na oblaku pristup je resursima računarstva kao što su aplikacije, poslužitelji, pohrana podataka, razvojni alati itd. koji su smješteni na udaljenom podatkovnom centru kojim upravlja pružatelj usluga u oblaku (engl. Cloud Service Provider - CSP). CSP pruža ove resurse uz mjesečnu pretplatu ili ih naplaćuje prema korištenju. Prednosti korištenja računarstva u oblaku su smanjenje troškova: oblak omogućuje smanjenje troškova i problema povezanih s kupnjom, instaliranjem, konfiguriranjem i upravljanjem lokalnom infrastrukturom, poboljšanje fleksibilnosti: uz oblak, organizacije mogu početi koristiti poslovne aplikacije za nekoliko minuta umjesto da čekaju tjedne da podrška odgovori, postavi hardver i softver te kupi podršku za instalaciju. Oblak omogućuje korisnicima, pogotovo programerima i znanstvenicima da sami upravljaju i poslužuju softver, lakše i jeftinije skaliranje: oblak omogućuje da umjesto kupnje viška

kapaciteta koji bi stajao neiskorišten, možete skalirati kapacitet prema potrebi, ovisno raste li promet ili pada. Također, možete koristiti mrežu svog pružatelja usluge u oblaku kako biste približili aplikacije korisnicima diljem svijeta [6].

Računarstvo na rubu distribuirana je tehnološka arhitektura gdje se podaci klijenata obrađuju na rubu mreže, što je bliže izvoru. Jednostavno rečeno, računarstvo na rubu premješta dio pohrane i dio resursa iz središnjeg podatkovnog centra bliže izvoru podataka. Umjesto slanja sirovih podataka u središnji podatkovni centar na obradu i analizu, obrada se odvija ondje gdje su podaci generirani, npr. tvornica, trgovina ili čak pametni grad. Samo rezultat obrade na rubu šalje se natrag u glavni centar radi daljnjih pregleda i obrada [7].

Softverski definirano umrežavanje (engl. software defined networking – SDN) pristup je mrežnoj arhitekturi koji omogućuje inteligentno i centralizirano upravljanje mrežom pomoću softvera. To pomaže operaterima da dosljedno i sveobuhvatno upravljaju mrežom. Pomoću *SDN*-a, mrežno ponašanje može se centralno programirati pomoću aplikacija koje koriste otvorene *API*-je [8].

Virtualizacija mrežnih funkcija (engl. software function virtualization – NFV) način je virtualizacije mrežnih usluga kao što su vatrozidi i usmjerivači koji tradicionalno rade na hardveru. Ove usluge pakirane su kao virtualni strojevi na standardnom hardveru koji omogućuju pružateljima usluga da pokreću svoju mrežu na poslužiteljima umjesto prilagođenih uređaja. Korištenjem *NFV*-a nije potrebno imati hardver za svaku mrežnu funkciju. *NFV* doprinosi skalabilnosti i fleksibilnosti jer dopušta davateljima usluga implementaciju novih mrežnih usluga bez potrebe za dodatnim hardverskim resursima [9].

Segmentacija mreže (engl. network segmentation) arhitekturalni je pristup u kojem se mreža dijeli na više segmenata ili podmreža gdje svaka djeluje kao vlastita mala mreža. To mrežnim administratorima omogućuje kontrolu protoka mrežnog prometa između podmreža na temelju pravila. Organizacije koriste segmentaciju mreža radi poboljšanja nadzora, povećanja učinkovitosti, identificiranja tehničkih problema te poboljšanja sigurnosti [11].

Komunikacija uređaja do uređaja (engl. device to device communication – D2D) nova je paradigma u mobilnim mrežama. Ona omogućuje uređajima korisnika u blizini da komuniciraju koristeći izravnu vezu umjesto odašiljanja radio signala kroz baznu stanicu ili jezgru mreže. Glavna prednost *D2D* komunikacije je vrlo niska latencija u komunikaciji zbog kratkog puta signala. Bežične tehnologije kratkog dometa, npr. *Bluetooth*, *WiFi Direct*, *LTE Direct* itd. mogu se koristiti za omogućavanje *D2D* komunikacije. *D2D* operatorima omogućuje više fleksibilnosti za rasterećenje prometa jezgre mreže, povećanje spektralne učinkovitosti, smanjenje potrošnje energije i cijene po bitu [10].

### 3. PRIMJENA *BLOCKCHAIN* TEHNOLOGIJE U 5G SUSTAVIMA

U ovom dijelu detaljno je objašnjeno kako se *blockchain* može integrirati s nekima od ključnih tehnologija koje omogućavaju 5G te primijeniti u dijeljenju 5G infrastrukture, međunarodnom roamingu, segmentiranju mreže i masovnoj podršci.

#### 3.1. *BLOCKCHAIN* ZA RAČUNARSTVO U OBLAKU

U računarstvu u oblaku, *blockchain* može stvoriti decentraliziranu mrežu čvorova koji dijele podatke i računalnu snagu. To omogućuje organizacijama da izbjegnu korištenje središnjeg pružatelja usluga. Umjesto toga, mogu se osloniti na distribuiranu mrežu računala koja nije pod utjecajem nikakve organizacije. Ovakav sustav može pružiti nekoliko korisnih stvari: povećanu sigurnost, povećanu skalabilnost i povećanu dostupnost. *Blockchain* također omogućuje razvoj novih aplikacija koje trenutačno nisu moguće s tradicionalnom arhitekturom temeljenom na oblaku. Na primjer, decentralizirana mreža čvorova može se koristiti za stvaranje sigurnijeg i otpornijeg sustava za distribuiranu pohranu datoteka. Glavna upotreba *blockchaina* u računarstvu u oblaku povezana je s internetom stvari. Internet stvari veza je uređaja i objekata s internetom. To uključuje sve, od povezanih automobila pa do kućanskih aparata. Internet stvari generira ogromnu količinu podataka koja se mora pohraniti, obraditi te analizirati. Mnoge industrije koriste internet stvari za prikupljanje podataka s povezanih uređaja u razne svrhe kao što su praćenje imovine i upravljanje inventarom. Predviđa se da će se broj *IoT* uređaja diljem svijeta popeti na 29 milijardi do 2030. godine.

Upotreba *blockchaina* u računarstvu u oblaku može pomoći tvrtkama da bolje upravljaju podacima i osiguraju ih. Na primjer, sustav temeljen na *blockchainu* može se koristiti za sigurnu i zaštićenu pohranu podataka prikupljenih *IoT* uređaja.

U *blockchain* baziranoj infrastrukturi oblaka, svaki čvor u mreži drži kopiju *blockchaina*. Kada se nova transakcija doda u *blockchain*, svi se čvorovi mreže ažuriraju novim informacijama. Ovo omogućuje decentraliziran, transparentan i siguran način rukovanja podacima.

Koristi *blockchaina* u računarstvu u oblaku su:

- Poboľjšana sigurnost – jedna od najvećih prednosti korištenja *blockchaina* je to što je on izuzetno siguran. Pomoću *blockchaina*, podaci su pohranjeni u čvorove diljem mreže umjesto na samo središnjoj lokaciji.

- Povećana skalabilnost – *Blockchain* može biti lako skaliran da obuhvati više korisnika i transakcija jer je distribuirana baza podataka. Na primjer, ako tvrtka želi proširiti svoju mrežu temeljenu na oblaku da ima više korisnika, može dodati više računala u mrežu.
- Poboljšana efikasnost – *Blockchain* može pomoći u poboljšanju efikasnosti u mrežama temeljenima na oblaku. Pošto je *blockchain* distribuirana baza podataka, može se smanjiti broj posrednika što omogućuje ubrzanje transakcija i poboljšanje ukupne efikasnosti mreže.
- Poboljšana mogućnost praćenja – *Blockchain* bilježi i pohranjuje svaku transakciju u javni registar. Mogućnost praćenja vrlo je važna za organizacije koje se bave osjetljivim podacima, na primjer zdravstvo i financije. Praćenjem svake transakcije, tvrtke mogu biti sigurne da će podaci biti povjerljivi i sigurni.
- Smanjeni troškovi – eliminiranjem posrednika, *blockchain* može pomoći u eliminiranju administrativnih troškova. *Blockchain* je također više automatiziran nego tradicionalne mreže, što može još više pomoći u smanjenju troškova [12].

Nekoliko primjera korištenja *blockchaina* u računarstvu u oblaku su:

- Zdravstvo – U zdravstvu barata se osjetljivim podacima pacijenata i centralizirana baza podataka čini ih lakom metom za hakere. *Blockchain* temeljena aplikacija za zdravstvo pomogla bi u eliminiranju ovakvih rizika enkripcijom i decentraliziranjem podataka pacijenata. Takav sustav znatno bi otežao hakerima bilo kakav pristup i izmjenjivanje podataka pacijenata. *Blockchain* bi također mogao pomoći u pravljenju sigurnih medicinskih dijagnoza, liječenja i procedura. Ovo može olakšati praćenje medicinske povijesti pacijenata i onemogućiti prevare i greške [23].
- Bankarstvo – Bankarstvo je sektor u kojem je sigurnost najvažnija stvar. Bankarstvo također može osigurati podatke korisnika koristeći *blockchain* temeljene aplikacije. Na primjer, identitet korisnika može se verificirati njihovim digitalnim potpisom. *Blockchain* se također može koristiti za spremanje svih transakcija gdje samo korisnici kojima se vjeruje mogu imati čvorove za provjeru valjanosti što onemogućuje jednu točku napada koja bi ugrozila čitav sustav [24].
- Automatizacija pametnog doma – Automatiziranjem uređaja u kući možemo ju pretvoriti u pametni dom i donijeti pogodnosti za ljude koji žive ondje. Pametni dom sastojao bi se od *IoT* uređaja kao što su detektori i senzori koji prikupljaju informacije iz svog okruženja, spremaju ih na oblak, ondje ih procesiraju te na temelju toga vrše predefiniranu radnju. Na

primjer, senzori za temperaturu detektiraju požar u kući te pohranjuju podatke na oblak, procesiraju ih te onda upale prskalice ili obavijeste vlasnika. U pametnim domovima može se iskoristiti automatizirani *blockchain* koji bi smanjio rizik gubitka podataka i osigurao im privatnost. Decentralizirana arhitektura *blockchaina* mogla bi osigurati sigurnost i stabilnost cijelog sustava [25].

### **3.2. BLOCKCHAIN ZA 5G DIJELJENJE INFRASTRUKTURE**

S vremenom, potražnja za mobilnim podatkovnim prometom sve je veća i veća. Kako bi se zadovoljio taj porast, 5G mreže pružaju povećanje kapaciteta sustava za čak 1000 puta, smanjuju kašnjenje prijenosa podataka te poboljšavaju performanse za korisnike na rubu ćelija. Kako bi se postigli ovakvi ciljevi, operateri mobilnih mreža razmatraju izgradnju guste mreže s mnogo malih ćelija. Međutim, takva gusta mreža rezultira većim vlasničkim troškovima. Samoupravljajuća mreža (engl. Self-Organizing Network - SON) može smanjiti troškove takvih mreža pomoću samo-konfiguracije, samo-optimizacije i samo-iscjeljivanja. Iako operateri mogu smanjiti troškove upravljanja i održavanja pomoću *SON* algoritma, on još nije do kraja istražen. Jedan primjer upotrebe za *SON* je omogućiti operateru da dijeli svoju mobilnu mrežu s drugim operaterima, čime se smanjuju troškovi ulaganja u infrastrukturu operatera. Postoji nekoliko rješenja koja omogućuju dijeljenje mrežnih resursa, lokacije, stupova, radio pristupne opreme i roaminga. U današnjim arhitekturama, mrežni operateri koriste model dogovora poznat kao sporazum o razini usluge (engl. service level agreement - SLA). *Blockchain* može djelovati kao faktor koji olakšava dijeljenje mrežnih resursa između operatera na autonoman i siguran način. Dodatno, pomoću pametnih ugovora pokazano je kako operateri mogu dijeliti svoje mrežne resurse preko *peer-to-peer* transakcija koje su slične *SON*-u, ali imaju distribuirani pristup.

Podaci o pretplati korisnika i autentikacijski ključevi mogu se pohraniti u distribuiranu knjigu, a ne u centralizirani poslužitelj za domaće pretplatnike (engl. home subscriber server – HSS) i postupci provjere autentičnosti i sigurnosti mogu biti napravljeni pomoću glavne knjige. Može se koristiti nova arhitektura za jezgru mreže gdje će se umjesto središnje baze podataka koja čuva sve podatke pretplatnika na jednom mjestu, koristiti distribuirana baza podataka. Postoji nekoliko načina za pohranu podataka u distribuiranu bazu podataka temeljenu na *blockchain* tehnologiji. Informacije se mogu direktno skladištiti u samom *blockchainu*. Iako je to najlakši način pohrane informacija, povlači za sobom sporost transakcija. Ovaj nedostatak može dovesti do problema u

dohvaćanju informacija korisnika, pogotovo u slučajevima prijenosa između malih ćelija. Stoga je potrebno imati distribuiranu bazu podataka s brzim transakcijama. Jedna od mogućnosti je međuplanetarni sustav datoteka (engl. Interplanetary File System – IFS), tehnologija temeljena na *BitTorrentu* koja se koristi jer ima ogroman kapacitet za podatke i vrlo veliku brzinu transakcija. Jezgra mreže svih mobilnih operatera treba imati pristup takvoj distribuiranoj bazi podataka te omogućiti operaterima pružanje usluga čak i pretplatnicima drugih operatera na temelju uspješne autentifikacije. U ovom scenariju, dobro je koristiti konzorcijalni *blockchain* za omogućavanje suradnje među različitim operaterima. Konzorcijalni *blockchain* omogućio bi da više operatera mogu djelovati kao administratori koji odlučuju, odobravaju i odabiru povezane čvorove u lancu na temelju dozvola. Također, konzorcijalni *blockchain* dosta je sigurniji od javnog *blockchaina* i onemogućuje neke vrste napada koji su ondje mogući, na primjer sibilski napad (engl. sybil attack). Osim toga, korištenje energetski zahtjevnog mehanizma konsenzusa nije praktično zbog velikih operativnih troškova, stoga su dokaz o udjelu i delegirana bizantska tolerancija na greške najbolje opcije. Pretpostavljeno je da su sve jezgre mreže različitih operatera dio konzorcijalnog *blockchaina* pa svaka od njih može komunicirati s pametnim ugovorom preko transakcije na adresu pametnog ugovora. Budući da administrator autentificira svaki čvor kao dio *blockchaina*, svi čvorovi imaju kopiju cijelog *blockchaina*.

Kada operater postavi novu SIM karticu, informacije o SIM kartici distribuiraju se u konzorcijalnom *blockchainu* preko novog bloka. Dalje se mogu stvarati novi blokovi i cijeli se *blockchain* ažurira novim pretplatama i potrošnjom podataka. Svaki put kada korisnik obavi neku radnju, npr. nova pretplata, te informacije pohranjene su u drugi blok i nakon što ih drugi čvorovi odobre, objavljene su svim ostalim čvorovima unutar lanca kao kopija u distribuiranom registru. Taj registar će za razliku od klasične arhitekture, ostati dijeljen među svim operaterima. Kada se SIM kartica prvi puta proda klijentu, operater provjerava klijenta te šalje šifrirani dokaz u *blockchain*. Pametni ugovor poslije toga provjerava pripada li taj korisnik nekom od operatera koji već imaju sporazum s konzorcijalnim *blockchainom*. Ako imaju, pametni ugovor šalje ključeve za autentikaciju entitetu za upravljanje mobilnošću. Entitet zatim provodi autentikacijske i sigurnosne mehanizme prema korisničkoj opremi. Nakon završetka, entitet traži i prima podatke o pretplati od distribuiranog registra. Poslije toga entitet uspostavlja potrebne radioveze kako bi pružio usluge korisniku. Kada se korisnik odvoji od mreže, entitet šalje podatke korisnika o naplati u pametni ugovor. Nakon toga, pametni ugovor provjerava pripada li korisnik servisnom operateru ili gostujućem operateru. Ako pripada servisnom, kreira se novi blok s ažuriranim informacijama o korisnikovoj pretplati. Ako pripada gostujućem, uz ažuriranje korisničkih podataka u novom



bloku, obavlja se *peer-to-peer* transakcija između novčanika operatera domaćina i novčanika operatera usluge putem pametne potrošnje ugovora temeljene na korisniku i sadržaja pametnog ugovora. Sadržaj pametnog ugovora također se može mijenjati s vremena na vrijeme ovisno o zemljopisnom položaju ćelija. Na primjer, male ćelije na prepunim lokacijama (npr. gradskim središtima) mogu zahtijevati više kriptovaluta nego male ćelije u udaljenim područjima. Ove informacije se mogu unaprijed dogovoriti između operatera [13].

### **3.3. PRIMJENA *BLOCKCHAINA* U MEĐUNARODNOM ROAMINGU**

Međunarodni roaming jedna je od mnogih ključnih usluga koje mobilni operater omogućuje na SIM karticama svojih korisnika, omogućujući im obavljanje poziva, slanje poruka i korištenje mobilnih podataka i interneta kada putuju u drugu zemlju. To je zapravo plaćeno „proširenje“ prilagođenih podatkovnih usluga iz matične mreže na zemlju koju posjećujete. Taj servis za „proširenje“ omogućen je pomoću sporazuma o roamingu između matičnog operatera korisnika i operatera zemlje koju posjećuju. Svi tehnički i komercijalni elementi potrebni da bi produljenje bilo moguće obuhvaćeni su roaming ugovorom.

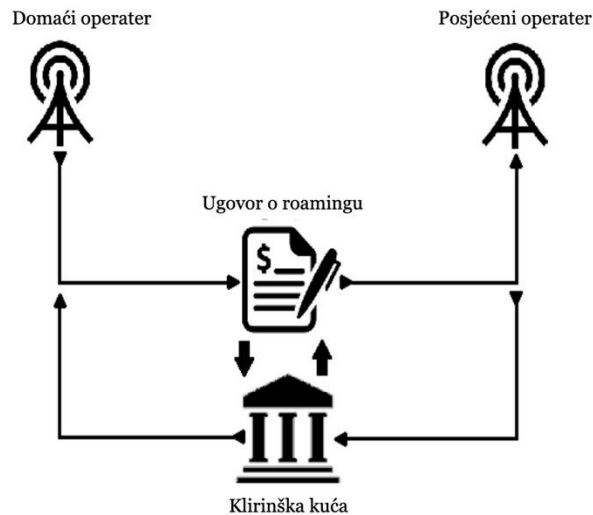
Većina međunarodnih roaming usluga naplaćuje korisnicima velike cijene kako bi pokrili troškove koje domaći operater ima prilikom sklapanja ugovora o roamingu s operaterom zemlje koju posjećuju. Ugovori se mogu razlikovati u cijeni od jednog ugovora do drugog. Ova razlika se događa zbog decentralizirane prirode pridržavanja operatera svojim nacionalnim propisima. Stoga je potrebna pomoć klirinških kuća kako bi upravljale sporazumima između operatera i rješavale eventualne sporove koji mogu nastati.

Najčešće rješenje ljudima je kupiti lokalnu SIM karticu države koju posjećuju ili međunarodnu SIM karticu koja pokriva države koje misle posjetiti, ali razlika u odnosu na međunarodni roaming je vrlo mala i javlja se problem što napraviti sa SIM karticom nakon povratka u državu. Trenutno su troškovi međunarodnog roaminga vrlo veliki jer se dogovori između operatera oslanjaju previše na klirinške kuće koje djeluju kao posrednici. Dogovori oko roaminga se također često mijenjaju zbog regulacija što dovodi do smanjenja kvalitete i povećanja cijena što korisnici moraju prihvatiti jer nemaju drugih opcija. Primjenom *blockchaina*, ovi problemi mogli bi se riješiti.

Trenutna usluga međunarodnog roaminga temelji se na odnosu između operatera koji se temelji na centraliziranoj bazi podataka. Ova središnja baza podataka sastoji se od dva ključna elementa:

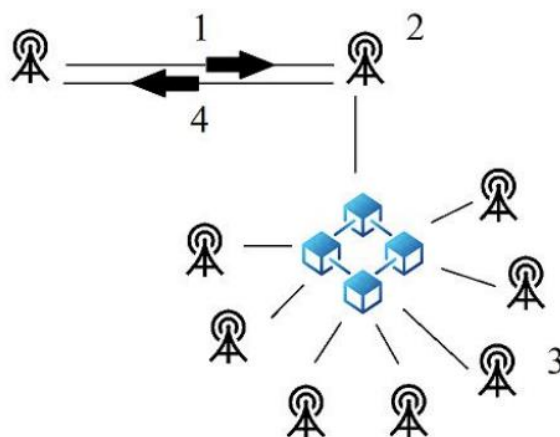
ugovora o roamingu i klirinških kuća. Shema je prikazana na slici 3.1. Roaming ugovori reguliraju obveze domaćeg operatora i operatora posjećene zemlje u davanju korisniku pristupa međunarodnoj roaming usluzi.

Klirinške kuće osiguravaju da se obje strane pridržavaju svojih obveza te riješe moguće probleme. Iako je ovakav sustav učinkovit, on može rezultirati većim cijenama. Ovaj problem se može riješiti uporabom *blockchain* tehnologije.



Slika 3.1. Shema međunarodnog roaminga između 2 operatera [14]

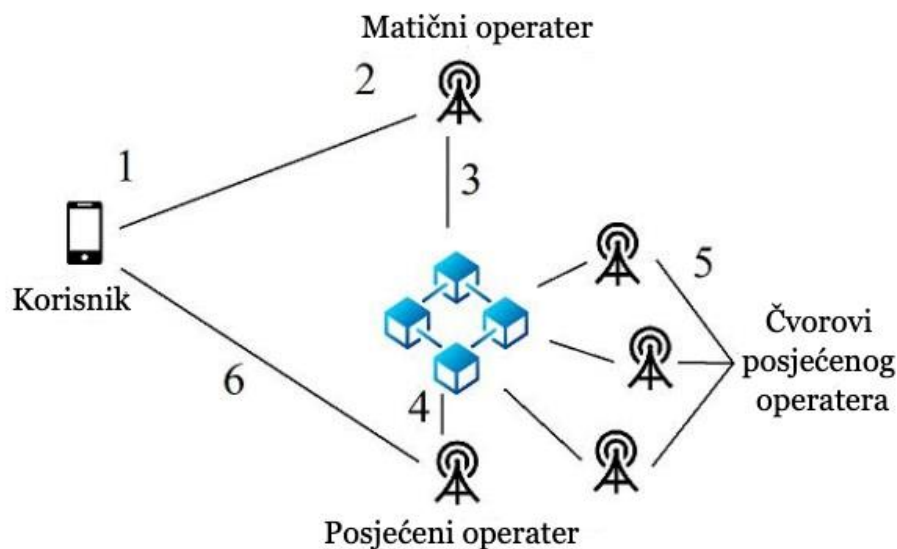
U radu [14] predložena je shema sa *blockchainom* koja se sastoji od dva važna dijela; registracije operatera u *blockchain* mrežu i korisnikov upit za međunarodni roaming.



Slika 3.2.. Registracija operatera u blockchain [14]

Svaki operater mora biti registriran u *blockchain* mrežu. Koraci I. – IV. odgovaraju koracima 1 – 4 na slici 3.2. U ovom primjeru nalazi se devet operatera. Osam ih je registrirano, a deveti mora proći kroz postupak registracije kako bi postao dio mreže:

- I. Operater zainteresiran za pridruživanje u *blockchain* mrežu šalje zahtjev najbližem operateru koji je dio *blockchain* mreže. Ovisno o čvorovima-članovima mreže za provjeru, zahtjevi će se razlikovati po tome što traže od zainteresirane strane.
- II. Najbliži operater dobiva zahtjev i gura ga u mrežu zajedno sa njegovim digitalnim *hashom* i identitetom. Taj operater postaje podnositelj zahtjeva za uvođenje novog bloka u mrežu.
- III. Svi čvorovi glasaju sukladno sa podnesenim zahtjevima. Moraju se zadovoljiti pravila prije glasanja i prije potvrde kako bi blok bio prihvaćen u mrežu.
- IV. Nakon glasanja, operater koji je prvi dobio zahtjev će poslati poruku zainteresiranom operateru koja sadržava njegov digitalni *hash* i identitet ako je prihvaćen u *blockchain* mrežu.



Slika 3.3. Registracija korisnika u međunarodni roaming servis [14]

Korisnik se također mora registrirati za korištenje međunarodne roaming usluge. Koraci I. – VI. Odgovaraju koracima 1- 6 na slici 3.2. i objašnjavaju registracijski postupak:

- I. Korisnik omogućuje roaming na svojem uređaju pa se zahtjev sa spajanje šalje matičnom operateru. Ako nemaju ugovor, kada se roaming uključi, operateru će se odmah poslati

identitet, *hash*, profil i država koju korisnik posjećuje te račun koji će biti naplaćen kada se uspostavi ugovor.

- II. Matični operater provjerava postoji li već ugovor koji omogućuje roaming unutar mreže.
- III. Ako ne postoji, matični operater će proslijediti informacije drugom operateru. Nakon toga se ugovor pokreće i šalje dalje u *blockchain* mrežu gdje će se verificirati i odobriti.
- IV. Drugi operater verificira identitet i odlučuje hoće li odobriti pametni ugovor ili ne i šalje status ugovora *blockchain* mreži.
- V. Čvorovi drugog operatera obrađuju transakciju u *blockchain* mrežu. Nakon toga ažuriraju *blockchain* status i šalju ga preko *Tendermint* konsenzus mehanizma.
- VI. Drugi operater dodaje korisnikov profil u lokalnu mrežu i omogućava mu da pristupi njegovim servisima i resursima.

### **3.4. PRIMJENA *BLOCKCHAINA* U SOFTVERSKI DEFINIRANOM UMREŽAVANJU**

Softverski definirano umrežavanje postala je vrlo važna mrežna paradigma zbog povećanja složenosti upravljanja i konfiguriranja mreža. Softverski definirano umrežavanje omogućuje odvajanje mrežne kontrole od toka podataka što može napraviti mrežu programibilnom, fleksibilnijom i agilnijom za podršku virtualiziranog poslužitelja i pohrane u modernom podatkovnom centru. U softverski definiranom umrežavanju, mrežna inteligencija postavljena je u softver zvan *SDN* upravljač koji omogućuje mrežnim administratorima da dinamički optimiziraju, vode i osiguravaju resurse mreže i oblikuju obrasce mrežnog prometa. Iako je *SDN* vrlo koristan, uvodi nove sigurnosne prijetnje i nedostatke. Zbog agregacije cijelog mrežnog vođenja i konfiguracije u jedan *SDN* upravljač, on se može smatrati jednom točkom kvara. Također, *SDN* je slab na prijetnje kao što su lažni tokovi prometa, napadi na ranjivosti upravljača, unutrašnji napadi na distribuirane upravljače itd. Većina ovih prijetnji i problema može se riješiti integriranjem *SDN* i *blockchain* tehnologije [15].

U *blockchain* baziranom *SDN*-u nalaze se distribuirani upravljači koji povećavaju sigurnost po pitanju jedne točke kvara. Kontrolni i aplikacijski sloj mogu se pojednostavniti kao dvije velike komponente gdje se mogu implementirati sigurnosni mehanizmi. *Blockchain* se ovdje može iskoristiti za poboljšanje sigurnosti distribuiranih upravljača i raznih uređaja za prosljeđivanje u toku podataka.

Kako bi se ovaj okvir mogao implementirati, vrlo je važno napraviti strukturu između aplikacija, upravljača, sigurnosnih mehanizama i važnih interakcija. Istraženo i predloženo je mnogo struktura, a jedna od njih je *DistBlockNet*, *blockchain* bazirana sigurna *SDN* arhitektura za *IoT* mreže.

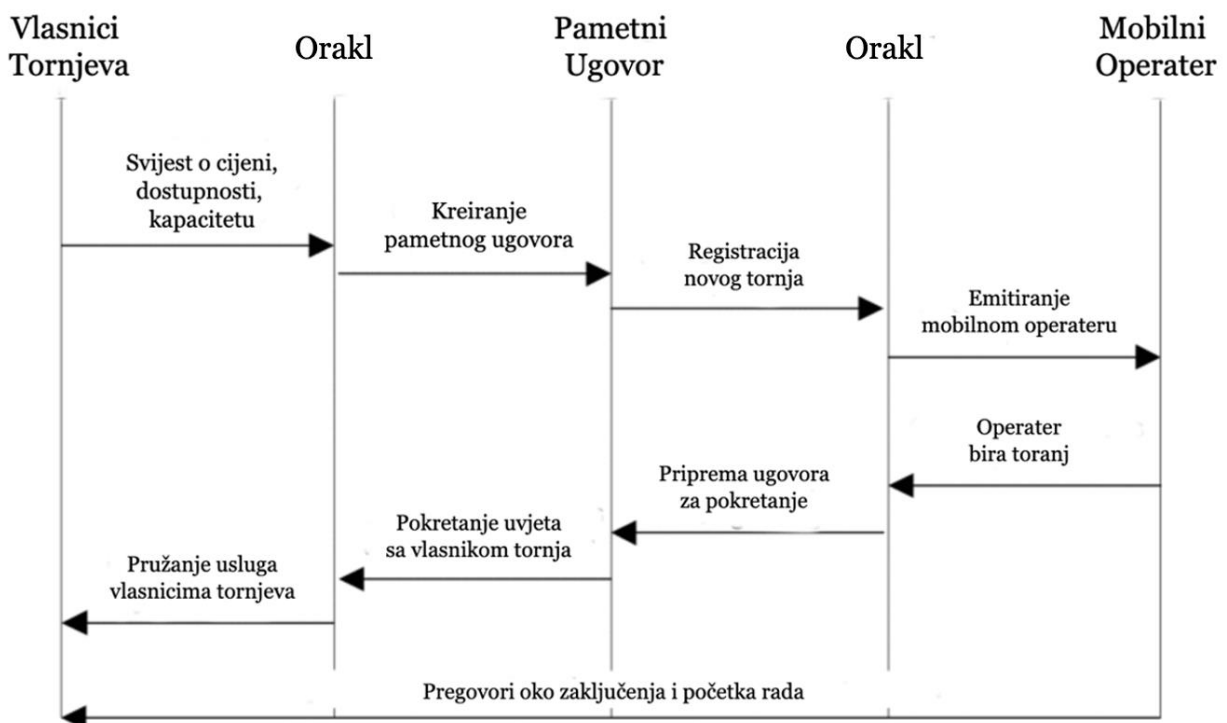
U *DistBlockNet* arhitekturi, svi upravljači u *IoT* mreži spojeni su međusobno na način distribuirane *blockchain* mreže tako da svi *IoT* uređaji za prosljeđivanje u mreži mogu jednostavno komunicirati. Sve lokalne mreže se sastoje od *OrchAppa*, upravljača i modula skloništa. Moduli skloništa i *OrchAppa* rješavaju sigurnosne prijetnje u svakoj lokalnoj mreži na različitim razinama. *OrchApp* radi na upravljanju aplikacijskih slojeva, upravljačko-aplikacijskom sučelju i kontrolnom sloju. Sklonište radi na podatkovnom sloju, upravljačko-podatkovnom sučelju i kontrolnom sloju. *DistBlockNet* arhitektura osim što omogućava veliku fleksibilnost, omogućava i aktivnu prevenciju problema umetanjem *OrchApp* modula i modula skloništa. *OrchApp* nudi mrežnu infrastrukturu koja je agilna, modularna i što je najvažnije, sigurna [16].

Prilikom integriranja *blockchaina* i *SDN*-a, nastala struktura može naslijediti različite pogodnosti i od *blockchaina* i od *SDN*-a kao što su:

- Prilagodljivost – pomoću *SDN* karakteristika, generički okvir je prilagodljiv kada se okruženje mijenja. Ovo je vrlo važno kako bi se osigurao rast cijele mreže kada raste broj pripadajućih uređaja.
- Dostupnost – okvir može osigurati visoku dostupnost, pogotovo za *SDN* upravljač u određenim scenarijima. Omogućuje korištenje *blockchaina* da štiti upravljač sa mehanizmima kao što je sklonište koje ga štiti od pretrpavanja napadima.
- Pouzdanost – za vrlo velike mreže, generički okvir može napraviti ravnotežu između postignutog i predviđenog učinka unutar različitih uvjeta.
- Skalabilnost – to je mogućnost upravljanja ili prilagođavanja mreže koja se proširuje. Zahvaljujući *SDN* upravljačima, generički okvir je fleksibilan i proširiv kada se broj uređaja u mreži poveća.
- Sigurnost – Generički okvir može osigurati mrežu od napada pomoću *blockchaina* i korištenjem adekvatnih sigurnosnih mehanizama.

### 3.5. BLOCKCHAIN ZA MASOVNU PODRŠKU 5G INFRASTRUKTURE

Masovna podrška infrastrukture omogućuje malim ulagačima u infrastrukturu da postave svoje mobilne tornjeve te da oni budu dio cijele infrastrukture operatora. Kako bi manji ulagači mogli postati dio operaterove infrastrukture, moraju biti registrirani, upravljani, dobiti certifikat te biti plaćeni prilikom korištenja njihovih tornjeva. Ovdje, *blockchain* može uz pomoć pametnih ugovora pomoći u procesu registracije tornjeva, upravljanju korištenih resursa te u procesu plaćanja. U radu [17] predloženo je korištenje pametnih ugovora s uvjetima sporazuma o razini usluge između pružatelja usluga malih mobilnih uređaja i telekom operatora. Pomoću kazni i poticaja mogu se osigurati poštena ponašanja između sudionika.



Slika 3.3. Dijagram slijeda korištenja pametnih ugovora i orakla za infrastrukturu za crowdsourcing [2]

Prema slici 3.3. vlasnici tornjeva mogu se registrirati tako što pruže pametnom ugovoru informacije kao što su cijena, hardver, kapacitet, dostupnost, reputacija itd. Kada vlasnik uspješno registrira svoj toranj, to se emitira kao *blockchain* događaj svim mobilnim operaterima. Nakon toga, mobilni operateri mogu birati koje tornjeve žele iznajmiti pa kreću pregovori između vlasnika tornjeva i mobilnih operatera. Nakon postignutih pregovora, sporazum se pomoću pametnih ugovora zapisuje u *blockchain* i plaćanje se izvršava automatski kripto kovanicama na temelju dogovorenih pravila o korištenju i potrošnji. Ako dođe do kršenja pravila, to otkriju orakli (engl.

oracles), aplikacije koje provjeravaju i prenose vanjske podatke (informacije pohranjene izvan lanca) u pametne ugovore i koje prate imate li povreda SLA uvjeta [26]. To će dovesti do nevažeće upotrebe i blokirati plaćanje te rezultirati lošom reputacijskom ocjenom danom vlasniku tornja.

### 3.6. PRIMJENA *BLOCKCHAINA* U SEGMENTACIJI MREŽE

Segmentacija mreže jedan je od koncepata koji se primjenjuje u 5G mrežama zbog sve većeg prometa mobilnih podataka. Temelji se na tehnologijama virtualizacije mrežnih funkcija i softversko definiranog umrežavanja kako bi se ostvarila fleksibilna mreža koja može riješiti sve potrebe sve većeg i većeg prometa. Pomoću segmentacije mreže, operateri mogu napraviti višestruke virtualne mreže na jednoj zajedničkoj fizičkoj infrastrukturi. Ovo pruža nove prilike mobilnim operaterima jer te virtualne mreže, zvane odsječci, mogu koristiti i drugi operateri što dovodi do efikasnog korištenja infrastrukture, jačanja kapaciteta i proširenja mreže.

Segmentacije mreže sastoji se od 4 dijela:

- Operater mobilne mreže koji postavlja i održava fizičku mrežu.
- Operater virtualne mobilne mreže koji nema svoju fizičku mrežu nego ju iznajmljuje od operatera mobilne mreže.
- Pružatelj usluga koji radi na vrhu mrežne infrastrukture prema unaprijed dogovorenim zahtjevima koje operater mobilne mreže i operater virtualne mobilne mreže potpišu u ugovoru.
- Vertikalna industrija koja se sastoji od skupa aplikacija koje su specifične za neki sektor u industriji. Ona koristi infrastrukturu kako bi pružila usluge krajnjim korisnicima.

U radu [18] predloženo je *blockchain* bazirano segmentiranja mreže koje bi imalo još nekoliko dijelova:

- Globalni pružatelj odsječaka (engl. Global Slice Provider – GSP) - Mapira sve zahtjeve za pružanjima resursa odgovarajućim odsječcima. Radi to pomoću *blockchain* baziranog sustava za nadmetanje koji omogućava svim operaterima koji imaju *GSP* da se nadmeću.
- Uparivač zahtjeva i resursa (engl. Request-Resource Matcher - RRM) – Mapira sve zahtjeve klijenata u prikladne odsječke. Tijekom primitka zahtjeva, provjerava može li trenutni pružatelj ispuniti te zahtjeve. Ako ne može, RRM se pretvara u posrednika i emitira zahtjev u *blockchain* te odabire najbolju ponudu operatera.

- *Blockchain* jedinica – Piše zahtjeve za upit resursa u *blockchain* i prima sve ponude.
- Orkestar lokalnih resursa (engl. Local Resource Orchestrator – LRO) – Donosi odluke o kreiranju i ažuriranju odsječaka.
- Višestruki-GPS orkestar resursa (engl. Multi-GSP Resource Orchestrator – MGRO) – Alocira prikladne resurse za traženi zahtjev ako je odabrana odgovarajuća ponuda

Također, rad [18] podijeljen je u nekoliko dijelova:

- Postavljanje – operater koji se želi pridružiti *blockchain* baziranoj segmentiranoj mreži mora nabaviti certifikat javnog ključa koji dijeli sa svim operatorima u mreži kako bi se pridružio. Nakon što se operateri dogovore i prihvate ga, on potpisuje digitalni ugovor u kojem su objašnjena pravila kojih se mora pridržavati i aktivnosti koje smije raditi.
- Zahtjev klijenta – Klijent šalje zahtjeve za uslugu svome mrežnom operateru. Svaki zahtjev mora sadržavati ID klijenta, uvjete, vremenski period za koji to treba i lokaciju gdje će se usluga obavljati. Kada orkestar lokalnih resursa dobije zahtjev, provjerava može li se usluga obaviti lokalno. Ako može, ide se odmah na pružanje usluge, a u slučaju da ne može, mora se prvo obaviti nadmetanje operatera
- Bitcoin bazirano nadmetanje – Ako usluga ne može biti obavljena lokalno, *RRM* zahtjeva i resursa enkapsulira zahtjev u zahtjev za ponudu i šalje ga *blockchain* jedinici koja ga upisuje u *blockchain*. *Blockchain* jedinice svih operatera uzimaju zahtjev za ponudu i predaju ih *RRM*-u. *RRM* provjerava mogu li se ti zahtjevi ispuniti, ako mogu, radi ponudu, potpisuje ju javnim ključem operatera koji je poslao zahtjev i šalje to *blockchain* jedinici. *Blockchain* jedinica dodaje transakciju u *blockchain*. *Blockchain* jedinica operatera koji je poslao zahtjev dohvaća sve transakcije i šalje ih *RRM*-u koji ih dekriptira pomoću svoga javnog ključa i odabire transakciju koja bi najviše odgovarala njegovom klijentu. Na kraju, operater koji je poslao zahtjev pravi pametni ugovor koji povezuje kupca sa operaterom koji će izvršiti uslugu.
- Pružanje usluga - U slučaju lokalnog pružanja usluge, *LRO* alocira resurse kako bi se moglo krenuti sa izvršavanjem usluge. Kada je klijent gotov sa korištenjem usluge, *RRM* pravi izvješće i šalje račun klijentu. Ako je pružanje usluge išlo preko drugog operatera, *MGRO* alocira resurse kako bi pružanje usluge moglo krenuti. Nakon izvršavanja usluge, *RRM* radi izvješće i račun te ih dodaje u *blockchain*. *Blockchain* jedinica operatera koji je poslao zahtjev dohvaća izvješće i račun i šalje ih *RRM*-u koji ih dalje prenosi klijentu.



- Raskid – Operater može napustiti *blockchain* baziranu segmentiranu mrežu emitiranjem poruke o raskidu preko *blockchaina*. Prije raskida, operator mora provjeriti i osigurati da nema nikakvih pružanja usluga u tijeku. Ostali operateri tada mogu raskinuti ugovor sa njime i upisati tu transakciju u *blockchain*. U slučaju kršenja pravila, mogu provjeriti izvješća te ako je potrebno, dati kaznu.

### 3.7. PRIMJENA *BLOCKCHAIN* TEHNOLOGIJE U 5G SIGURNOSNIM USLUGAMA

Naglim porastom prometa u 5G mrežama rezultiralo je i naglim povećanjem osjetljivih podataka koje uređaji i korisnici generiraju. Zbog toga je vrlo važno razviti dobre i sigurne mehanizme u 5G mrežama otporne na napade i prijetnje. *Blockchain*, poznat po svojim sigurnosnim prednostima, može pomoći u tome.

Kontrola pristupa vrlo je važna kako bi se osiguralo da korisnici koji nemaju dopuštenje ne mogu pristupiti resursima mreže. Pametni ugovori mogu pomoći kod osiguravanja kontrole pristupa da se zaštiti mreža od raznih prijetnji. U radu [19] objašnjena je kontrola pristupa koja koristi pametne ugovore koji provjeravaju prava pristupa za *IoT* mreže. Ondje, politika pristupa nalazi se na ugovoru koji se nalazi na *blockchainu* i taj ugovor potvrđuje korisnikov zahtjev. Za razliku od svih prijašnjih arhitektura kod kontrole pristupa koje koriste tijelo izvana koje bi obavilo potvrdu, kod *blockchain* baziranog pristupa kontrola se obavlja direktno između osobe koja traži pristup i centra podataka što bi rezultiralo nižom latencijom.

*Blockchain* se sve više istražuje za potrebe autentikacije kako bi se poboljšala zaštita 5G mreža. Korisnici moraju biti autenticirani kako bi se otkrila i spriječila sva maliciozna ponašanja prema mreži. *Blockchain* može pomoći pri upravljanju certifikata svojom sigurnom distribucijom informacija preko cijele mreže. 5G mreže podržavaju velik broj uređaja i čvorova što čini distribuciju i upravljanje javnih ključeva i certifikata puno težim. Trenutno, kućna mreža (engl. home network), jezgra 5G mreže, zadužena je za proces autentikacije. To može izazvati dva problema: problem kašnjenja jer kućna mreža treba razmijeniti dosta poruka sa mrežom jezgre kako bi dobila sve parametre potrebne za autentifikaciju i problem sigurnosti jer kućna mreža može biti meta napada i ako ti napadi uspiju, mogu izazvati probleme kao što je rušenje cijele mreže. U radu [20] pokazani su autentifikacija i protokol dogovora o ključu za 5G mreže bazirani na *blockchainu*.

Taj se koncept oslanja na *blockchain* tako da protokoli imaju sigurnosne značajke *blockchaina* i distribuciju baze podataka. Koncept koristi kriptografske tehnike kako bi se obranio od raznih napada kao što su napadi pretvaranja, napadi uskraćivanja resursa, čovjek u sredini itd. Ne koristi kućnu mrežu prilikom autentifikacije što ju čini više sigurnom. Prilikom dodavanja u postojeću infrastrukturu, koncept ne zahtijeva dodavanje novih fizičkih dodataka.

U konceptu, kućna mreža zadužena je za pokretanje *blockchaina* i inicijalizaciju mreže. Informacije o svakom čvoru u mreži registriraju se kao transakcije u blok. Kućna mreža dijeli *blockchain* preko svih mrežnih čvorova tako da kada nova korisnička oprema dođe, njena registracija i autentifikacija radi se između nje i mreže za posluživanje bez uplitanja kućne mreže. Sigurnosna svojstva *blockchaina*, *blockchain* verificiranje korisničke opreme a i verificiranje *blockchaina* korisničkom opremom onemogućavaju napade otmicom.

## 4. PREDNOSTI I NEDOSTACI PRIMJENE BLOCKCHAINA U 5G MREŽAMA

U ovom poglavlju navedene su sve prednosti i nedostaci korištenja blockchaina u 5G sustavima. Prvo su opisane sve prednosti i razlozi zašto ga koristiti, a zatim nedostaci i problemi na koje se može naići tijekom integracije.

### 4.1. PREDNOSTI *BLOCKCHAINA* U 5G MREŽAMA

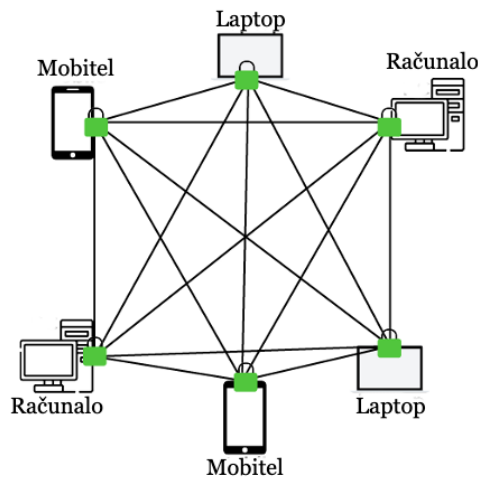
Blockchain može svojim svojstvima kao što su decentralizacija, nepromjenjivost, odgovornost itd. pomoći 5G mrežama u različitim aspektima i doprinijeti za:

- Poboljšanje sigurnosti – Sigurnost je jedna od najvažnijih stvari u 5G mrežama. *Blockchain*, uz pomoć svojih najpoznatijih svojstava, može pomoći u izgradnji sigurnijih 5G mreža. Uvođenjem decentralizacije, rješava problem centraliziranog vođenja mreža gdje treća strana provjerava i bilježi sve podatke i transakcije te može biti jedna točka napada. Uz *blockchain*, čak i ako je korisnik hakiran, sve operacije u mreži nastavljaju se normalno pomoću konsenzusa što osigurava da nema jedne točke napada i jamči bolju sigurnost. Također, uz pomoć pametnih ugovora, *blockchain* može uvesti decentraliziranu provjeru pristupa korisnika koristeći računalnu snagu ostalih valjanih korisnika u mreži što čini 5G usluge otpornijima na mijenjanje podataka.
- Automatizacija pomoću pametnih ugovora – Prema slici 4.1. vidi se da se pametni ugovori izvršavaju automatski, bez uplitanja treće strane, kada se uvjeti zadovolje za obje strane. Korisnici mogu razmjenjivati podatke i resurse pomoću pametnih ugovora u *blockchain* baziranim trgovinama. Pametni ugovori omogućiti će automatizaciju procesa sporazuma između tvrtki i korisnika, što će smanjiti vrijeme transakcija i administrativne troškove. Korisnici više neće ovisiti o središnjim autoritetima te morati plaćati veće cijene za njihove usluge nego će imati agenta koji će umjesto njih pregovarati o cijenama i uvjetima za usluge u realnom vremenu.



Slika 4.1. Način rada pametnih ugovora [27]

- Očuvanje privatnosti korisnika uz pomoć kriptografije – *Blockchain* može uz pomoć moderne kriptografije pomoći u očuvanju privatnosti korisnika. Također, ubacivanjem tehnologija kao što su protokol nultog znanja, digitalnih potpisa, homofornih enkripcija itd. možemo dodatno pojačati privatnost.
- Transparentnost i dostupnost – Svi čvorovi u *blockchainu* imaju pristup podacima i informacijama i javna knjiga dostupna je svima. Svaki korisnik ima kopiju glavne knjige spremljenu lokalno. Korisnici i klijenti mogu raditi transakcije i pristupati podacima sve dok su povezani sa aktivnim čvorom u *blockchainu*. Transparentnost podataka omogućiti će tvrtkama da analiziraju prošla ponašanja korisnika bez da se oslanjaju na zapise o njihovoj reputaciji što je vrlo važno za sve nove sudionike koji dolaze na tržište.
- Decentralizacija – Decentralizacija je ključna prednost *blockchaina*. Na slici 4.2. prikazan je izgled i povezanost decentralizirane mreže. *Blockchain* radi s decentraliziranim mehanizmom za provjeru valjanosti i odobravanja transakcija. Također, svaki čvor ima svoju lokalnu kopiju glavne knjige. Kod ovakvog pristupa, napadačima je puno teže preuzeti kontrolu nego kod centraliziranih pristupa. Također, svi blokovi transakcija su kriptografski povezani što ih čini teškima za izmjenu. Izbacivanjem centralizacije, *blockchain* se može iskoristiti za uspostavu izravne komunikacije između 5G pružatelja servisa i korisnika tako da bi se troškovi upravljanja mrežom mogli znatno smanjiti. Na primjer, mogao bi pomoći u uspostavi *D2D* komunikacije između korisnika koristeći računalnu snagu svih sudionika u mreži umjesto da se oslanjaju samo na treću stranu i tako bi mogao smanjiti troškove transakcija, smanjiti latenciju i omogućiti veću dostupnost svim korisnicima.



Slika 4.2. Decentralizacija u blockchainu

## 4.2. NEDOSTACI *BLOCKCHAINA* U 5G MREŽAMA

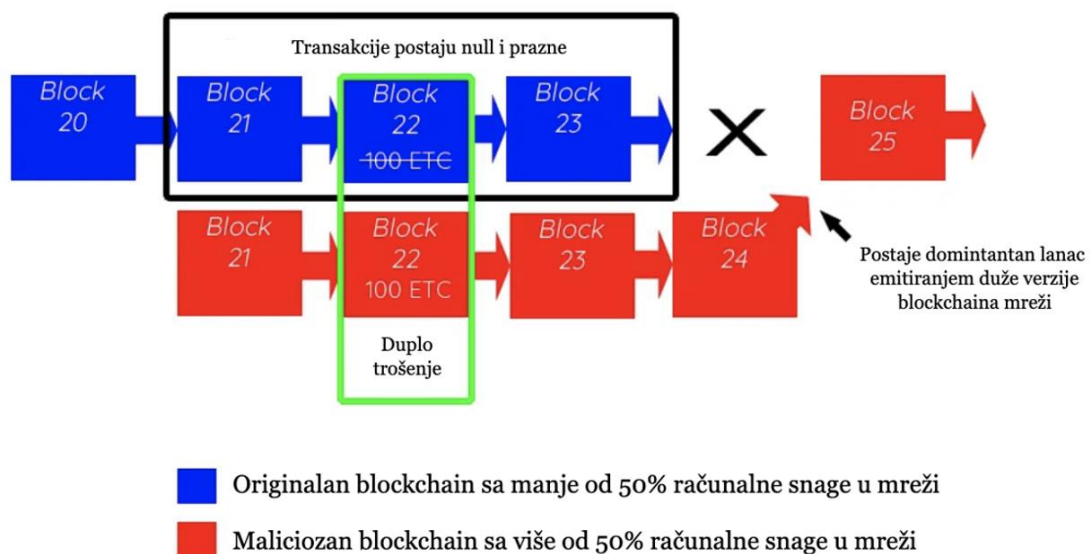
Iako se *blockchain* čini kao izvrsno rješenje te može revolucionirati 5G tehnologiju sa svojim svojstvima, nailazimo i na probleme koji se moraju pažljivo razmotriti, proučiti i riješiti prije implementiranja *blockchaina* u 5G sustave. Problemi su:

- Propusnost – Trenutno, skalabilnost je najveći problem prilikom integriranja *blockchaina* i 5G mreža. *Blockchain* ima puno manju propusnost u odnosu na druge aplikacije koje ne upotrebljavaju *blockchain*. Prema slici 4.3. *Bitcoin* ima propusnost do 7 transakcija po sekundi, dok na primjer *Visa* ima propusnost do 24000 transakcija po sekundi. Prije korištenja *blockchaina* u ogromnim količinama transakcija koje će generirati 5G aplikacije, moraju se pronaći rješenja za poboljšanje propusnosti kao što su nove *blockchain* arhitekture, povećanje veličina blokova, poboljšanje algoritama konsenzusa itd.



Slika 4.3. Usporedba broja transakcija po sekundi za različite aplikacije i kriptovalute [28]

- Skladištenje podataka – U *blockchainu*, svaki čvor mora imati kopiju glavne knjige koja se povećava svakom transakcijom. U *blockchain* 5G mrežama, *blockchain* će morati procesirati ogromne količine podataka koje će *IoT* uređaji konstantno slati. Ovo će zahtijevati velike količine pohrane koje će utjecati na performanse cijelog sustava
- Sigurnost – Iako se *blockchain* doima sigurnom bazom podataka, ima svoje slabosti koje se mogu iskoristiti u loše svrhe. Jedna od najvećih je 51% napad prikazan na slici 4.4. Ovaj napad može izvršiti napadač ili grupa napadača koji kontroliraju više od 50% rudarenja *hash*-a ili računalne snage u *blockchain* mreži. U tom slučaju, napadač može mijenjati transakcije i omesti proces dodavanja novog bloka. Izvođenjem 51% napada, napadač može manipulirati informacijama i izmjenjivati ih na *blockchainu*. Može izvesti napade kao što su poništavanje transakcija i iniciranje napada dvostrukog trošenja u kojem napadač troši iste novce dva ili više puta, može isključivati i izmjenjivati redoslijed transakcija, ometati rudarenje drugih rudara, sprječavati operaciju potvrde normalnih transakcija itd. Na ovome problemu se radi i već su donesena rješenja kao što je *SmartPool* koja čine ove napade gotovo nemogućima [21].



Slika 4.4. 51% napad (duplo trošenje) [29]

Također, sigurnost kod pametnih ugovora još je jedan problem. Kod u pametnim ugovorima može sadržavati računalne greške i ranjivosti koje napadači mogu iskoristiti. Kreiranje sigurnih i neranjivih 5G pametnih ugovora postalo je vrlo važno.

- Veliki troškovi – *blockchain* je skup po pitanju računalnih resursa jer mora rješavati složene probleme kod konsenzus algoritama. Također, sve operacije verificiranja

transakcija i generiranja blokova sadrže nekoliko kriptografskih operacija. Kod 5G-a, u slučaju ultra gustih mreža gdje su resursi jako ograničeni zbog velikog broja *IoT* uređaja, biti će jako teško pronaći dovoljno resursa za *blockchain* kako bi mogao obavljati sve operacije. Kod pametnih gradova, *IoT* uređaji generirati će ogromne količine podataka što će rezultirati velikim povećanjem veličine *blockchaina* što će mu otežati procesiranje velikih količina podataka. Bez dobrog dizajna, upotrebom *blockchaina* u 5G aplikacijama postoji rizik od velike potrošnje energije, duge latencije, može doći do zagušenja mreže i do visokih zahtjeva za propusnost.

- Privatnost – U Trenutnim 5G *IoT* sustavima, podaci se mogu spremati izvan lanca kod računarstva u oblaku kako bi se smanjio teret *blockchainu*. Takav način arhitekture može se iskoristiti tako da se napadač može pretvarati da je korisnik mreže i procesirati podatke u oblaku, ali da uz to uzima privatne podatke ostalih korisnika bez njihovog znanja što dovodi do ozbiljnih problema sa privatnošću. Pokazano je da u praksi zaštita podataka korisnika nije toliko čvrsta kod *blockchaina*. Iako *blockchain* koristi enkripciju i potpisivanje, svakom operacijom dio transakcije se otkrije svim korisnicima. Također, napadači mogu iskoristiti pametne ugovore i njihove mane kako bi došli do privatnih podataka ili privatnih ključeva korisnika. Kada se korisnik priključi *blockchain* mreži, sigurnost njegovih podataka ne može biti zajamčena. Zbog transparentnosti *blockchaina*, informacije, poput adresa pošiljatelja i primatelja, količine poslanih iznosa itd., dostupne su javno svim korisnicima u mreži.

## 5. ZAKLJUČAK

*Blockchain* je nova tehnologija koja postaje sve popularnija i proučavanija te koja će biti jedan od važnih dijelova 5G i budućih mreža ponajviše zbog svojih sigurnosnih svojstava, ali i potencijala da ubrza njihove performanse. U uvodu je prvo opisan *blockchain*; što je, na koji način radi, objašnjeni su najvažniji pojmovi i vrste *blockchaina* što nam je potrebno za daljnje razumijevanje rada. Zatim smo opisali 5G sustav i ključne tehnologije za omogućavanje 5G sustava. U glavnom dijelu, objasnili smo potencijalnu primjenu *blockchaina* u tehnologijama koje omogućuju 5G sustav i dijelovima 5G sustava, gdje *blockchain* pomoću decentralizacije, nepromjenjivosti, odgovornosti i pouzdanom pohranom podataka može potencijalno pomoći na različite načine u jačanju sigurnosti, privatnosti, stabilnosti, ubrzanju performansi i smanjenju troškova 5G sustava. Na kraju su objašnjene sve prednosti i nedostaci integracije *blockchaina* i 5G sustava i iako teoretski integracija izgleda korisno i primjenjivo, u praksi nije tako i mora se još puno poraditi na nedostacima *blockchaina*; najviše na njegovoj propusnosti, zauzeću memorije i velikim operativnim troškovima koji jako dolaze do izražaja u ogromnim količinama podataka kojima bi se moralo baratati prilikom integracije. Ovi nedostaci aktivno se istražuju i traže se rješenja koja bi mogla dovesti do isplative integracije u bliskoj budućnosti sa određenim tehnologijama i dijelovima 5G sustava.



## LITERATURA

- [1] Qualcomm, "What is 5G?," s Interneta, <https://www.qualcomm.com/5g/what-is-5g>, [13.9.2023].
- [2] A. Chaer, K. Salah, C. Lima, P. P. Ray and T. Sheltami, "Blockchain for 5G: Opportunities and Challenges" 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, pp. 1- 6, 2019.
- [3] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, "Blockchain for 5G and Beyond Networks: A State of the Art Survey," *Journal of Network and Computer Applications*, Vol. 166, pp. 1084-8045, 2020.
- [4] S. Rollins, "Consensus algorithms in Blockchain – Understanding the evolution of Blockchain Consensus Mechanisms," 2023., s Interneta, <https://blog.cryptostars.is/consensus-algorithms-in-blockchain-2d1653f294ce>, [13.9.2023].
- [5] Namasudra, S., Deka, G.C., Johri, P. *et al.* "The Revolution of Blockchain: State-of-the-Art and Research Challenges," *Arch Computat Methods*, Vol. 28, pp. 1497–1515, 2021.
- [6] IBM, "What is cloud computing?," s Interneta, <https://www.ibm.com/topics/cloud-computing>, [13.9.2023].
- [7] S. J. Bigelow, "What is edge computing? Everything you need to know," s Interneta, <https://www.techtarget.com/searchdatacenter/definition/edge-computing>, [13.9.2023].
- [8] Ciena, "What is SDN?," s Interneta, <https://www.ciena.com/insights/what-is/What-Is-SDN.html>, [13.9.2023].
- [9] Redhat, "What is NFV?," 2019., s Interneta, <https://www.redhat.com/en/topics/virtualization/what-is-nfv>, [13.9.2023].
- [10] U. N. Kar, D. K. Sanyal, „An overview of device-to-device communication in cellular networks“, *ICT Express*, Vol. 4, pp. 203 – 208, 2018.
- [11] Paloalto, „What is network segmentation?“, s Interneta, <https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation>, [13.9.2023].
- [12] R. Timbo, „Blockchain Cloud Computing: Benefits and Examples“, s Interneta, <https://www.revelo.com/blog/blockchain-cloud-computing>, [13.9.2023].
- [13] B. Mafakheri, T. Subramanya, L. Goratti and R. Riggio, "Blockchain-based Infrastructure Sharing in 5G Small Cell Networks," 14th International Conference on Network and Service Management (CNSM), Rome, Italy, pp. 313-317, 2018.
- [14] M. R. M. Bailon, L. Materum, „International Roaming Services Optimization Using Private Blockchain and Smart Contracts,” Vol. 8, No. 3, May 2019.

- [15] W. Li, W. Meng, Z. Liu, M. H. Au, "Towards Blockchain-Based Software-Defined Networking: Security Challenges and Solutions," Vol. 103, pp. 196 – 203, February 2020.
- [16] P. K. Sharma, S. Singh, Y. -S. Jeong and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," in *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78-85, Sept. 2017.
- [17] E. Di Pascale, J. McMenamy, I. Macaluso and L. Doyle, "Smart Contract SLAs for Dense Small-Cell-as-a-Service," March 2017.
- [18] M. A. Togou et al., "DBNS: A Distributed Blockchain-Enabled Network Slicing Framework for 5G Networks," in *IEEE Communications Magazine*, vol. 58, no. 11, pp. 90-96, November 2020.
- [19] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594-1605, April 2019.
- [20] Z. Haddad, M. M. Fouda, M. Mahmoud and M. Abdallah, "Blockchain-based Authentication for 5G Networks," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, pp. 189-194, 2020.
- [21] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco and P. Wightman, "The 51% Attack on Blockchains: A Mining Behavior Study," in *IEEE Access*, vol. 9, pp. 140549-140564, 2021.
- [22] A. Rosic, "Proof of Work vs Proof of Stake: Basic Mining Guide," s Interneta, <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>, [13.9.2023].
- [23] D. Trung, N. Ha, S. Le, H. Phan, Tan. "Smart Care: Integrating Blockchain Technology into the Design of Patient-centered Healthcare Systems," 105-109., 2020.
- [24] DBS, "Blockchain technology: transforming the future of banking," s Interneta, <https://www.dbs.com/blockchain/blockchain-technology-in-banking-how-are-banks-using-blockchain.html>, [13.9.2023].
- [25] M. Umer, S. Sadiq, R. M. Alhebsh, M. F. Sabir, S. Alsubai, A. A. Hejaili, M. M. Khayatt, A. A. Eshmawi, A. Mohamed, "IoT based smarthome automation using blockchain and deep learning models," s Interneta, <https://peerj.com/articles/cs-1332/>, [13.9.2023].
- [26] Ethereum, "Oracles," s Interneta, <https://ethereum.org/en/developers/docs/oracles/>, [13.9.2023].
- [27] P. Hooda, "Smart contracts in blockchain," s Interneta, <https://www.geeksforgeeks.org/smart-contracts-in-blockchain/>, [13.9.2023].

- [28] ResearchGate, “Cryptocurrencies speeds compared to Visa and Paypal,” s Interneta, [https://www.researchgate.net/figure/Cryptocurrencies-transaction-speeds-compared-to-Visa-and-Paypal-74\\_fig2\\_338792619](https://www.researchgate.net/figure/Cryptocurrencies-transaction-speeds-compared-to-Visa-and-Paypal-74_fig2_338792619), [13.9.2023].
- [29] A. Butler, “Ethereum classic attacked! How does 51% attack occur?,” 2019., s Interneta, <https://medium.com/hackernoon/ethereum-classic-attacked-how-does-the-51-attack-occur-a5f3fa5d852e>, [13.9.2023].

## SAŽETAK

U ovom radu opisane su potencijalne primjene *blockchain* tehnologije u dijelovima i tehnologijama 5G sustava. U uvodu su objašnjeni najvažniji koncepti, pojmovi, tehnologije i svojstva *blockchaina* i 5G sustava koji su važni za daljnje razumijevanje rada. U glavnom dijelu, objašnjena je potencijalna primjena *blockchaina* u računarstvu u oblaku, 5G dijeljenju infrastrukture, međunarodnom roamingu, definiranju mreža softverom, 5G infrastrukturi za *crowdsourcing*, segmentaciji mreže i 5G sigurnosnim uslugama. Nadalje, objašnjene su prednosti koje *blockchain* može donijeti prilikom integracije sa 5G sustavima, a zatim i nedostaci koje povlači za sobom i koji se aktivno rješavaju prije nego što se može krenuti sa integracijom.

Ključne riječi: *blockchain*, 5G sustav, računarstvo u oblaku, dijeljenje infrastrukture, međunarodni roaming, definiranje mreža softverom, *crowdsourcing*, segmentacija mreže

# **APPLICATION OF BLOCKCHAIN TECHNOLOGY IN 5G SYSTEMS**

## **ABSTRACT**

In this work, potential uses of blockchain technology in parts and technologies of 5G systems were explained. In the introduction, the most important concepts, terms, technologies and properties of blockchain and 5G systems which are important for further understanding of the work were explained. In the main part, potential use of blockchain in cloud computing, 5G infrastructure sharing, international roaming, software defined networking, 5G infrastructure for crowdsourcing, network segmentation and 5G security services was explained. Further, advantages which blockchain can bring during integration with 5G systems, and then disadvantages which it brings with itself and are actively being solved before we can start with the integration were explained.

Keywords: blockchain, 5G system, cloud computing, infrastructure sharing, international roaming, software defined networking, crowdsourcing, network segmentation

## ŽIVOTOPIS

Mihael Ećimović rođen je 17. rujna 2001. godine u Slavonskom Brodu. Završio je osnovnu školu Ivana Brlić Mažuranić u Budainci nakon čega je upisao matematičku gimnaziju Matija Mesić u Slavnskome Brodu. Nakon završetka gimnazije, upisuje preddiplomski sveučilišni studij računarstva na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija Osijek. Mihael trenira karate od 5. godine i aktivan je član hrvatske reprezentacije i trener mlađoj djeci. Od Siječnja 2023. radi u američkoj tvrtki *Wonderful Machine* gdje trenutno obučava sve nove zaposlenike.