Tehnologija lanca blokova u e-poslovanju

Gosić, Edin

Professional thesis / Završni specijalistički

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:168:104499

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-15**

Repository / Repozitorij:

FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repozitory

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Edin Gosić

TEHNOLOGIJA LANCA BLOKOVA U E-POSLOVANJU

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Edin Gosić

BLOCKCHAIN TECHNOLOGY IN E-BUSINESS

SPECIALIST THESIS

Zagreb, 2023.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija „Informacijska sigurnost“.

Mentor: Prof. dr. sc. Boris Vrdoljak

Specijalistički rad ima: 110 stranica

Specijalistički rad br.:_____

Povjerenstvo za ocjenu u sastavu:

1. doc. dr. sc. Luka Humski – predsjednik povjerenstva
2. prof. dr. sc. Boris Vrdoljak – mentor
3. prof. dr. sc. Ivan Magdalenić, Sveučilište u Zagrebu, Fakultet organizacije i informatike – član

Povjerenstvo za obranu u sastavu:

1. doc. dr. sc. Luka Humski – predsjednik povjerenstva
2. prof. dr. sc. Boris Vrdoljak – mentor
3. prof. dr. sc. Ivan Magdalenić, Sveučilište u Zagrebu, Fakultet organizacije i informatike – član

Datum obrane: 10. studenog 2023.

SAŽETAK

Tehnologija lanca blokova još uvijek se smatra novom tehnologijom, koja je u ranoj životnoj fazi. Njezin je potencijal velik i nadmašuje trenutačnu primjenu, a zbog sigurnosti može doprinijeti digitalizaciji procesa i sustava izvan svijeta kriptovaluta. Kao i kod svake nove tehnologije, na početku korištenja tehnologije uvijek je fokus na prednostima, dok sigurnosni aspekti tehnologije padaju u drugi plan. Cilj ovog rada je istražiti mogućnosti primjene tehnologije lanca blokova u elektroničkom poslovanju, s fokusom na sigurnosne aspekte sustava temeljenih na tehnologiji lanca blokova. Rad se sastoji od teorijskog dijela u kojem je opisana tehnologija lanca blokova, dijela u kojem su obrađene studije slučajeva napada na sustave koji koriste lanac blokova i dijela u kojem je izrađena analiza rizika tehnologije lanca blokova i u kojem je analizirana aplikacija lažni mobilni novčanik.

Ključne riječi: *lanac blokova, e-poslovanje, elektroničko poslovanje, informacijska sigurnost*

SUMMARY

Blockchain technology is still considered a new technology in its early stages. The technology has great potential, surpassing even current applications and due to its inherent security, facilitates the digitization of processes and systems beyond cryptocurrencies. As with any new technology and its use, the focus is always on the benefits while the security aspects fall into the background. This paper aims to investigate the possibilities of applying blockchain technology in electronic business, focusing on the security aspects of blockchain-based systems. The paper consists of a theoretical part describing blockchain technology, in which case studies present attacks on systems that use blockchain and a section on blockchain technology risk assessment where a fake mobile wallet application is analyzed.

Keyword: *blockchain, e-business, electronic business, information security*

Sadržaj

1. Uvod ... 1
2. Tehnologija lanca blokova ... 3
   2.1 Protokoli i algoritmi lanca blokova ... 6
      2.1.1 Dokaz o radu (PoW) ... 7
      2.1.2 Dokaz o udjelu ... 9
   2.2 Vrste tehnologije lanca blokova ... 11
   2.3 Kriptografija u lancu blokova ... 14
      2.3.1 Sažimanje ... 16
      2.3.2 Asimetrično šifriranje ... 17
      2.3.3 Merkleovo stablo ... 19
   2.4 Privatnost, sigurnost i povjerenje u lancu blokova ... 20
      2.4.1 Pametni ugovor ... 21
      2.4.2 Lanac blokova i zakoni ... 24
3. Primjena lanca blokova u e-poslovanju ... 27
   3.1 Lanac blokova i kriptovalute ... 27
   3.2 Lanac blokova i e-uprava ... 28
   3.3 Lanac blokova u zdravstvenom sustavu ... 32
   3.4 Lanac blokova u financijskom sustavu ... 35
      3.4.1 Sigurnost i transparentnost ... 36
      3.4.2 Smanjenje troškova ... 37
      3.4.3 Učinkovita kontrola rizika ... 37
      3.4.4 Instant transakcija ... 38
      3.4.5 Kvalitetnija financijska revizija ... 38
   3.5 Lanac blokova u sektoru prodaje ... 38
   3.6 Lanac blokova u B2B poslovnom sustavu ... 41
4. Slabosti, ranjivosti i napadi na lanac blokova ... 45
   4.1 Slabosti lanca blokova ... 45
   4.2 Ranjivosti lanca blokova ... 47
   4.3 Vrste napada i studije slučajeva ... 49
      4.3.1 Exchange napad ... 49

4.3.2 DeFi napad ... 53
4.3.3 51% napad ... 59
4.3.4 Phishing napad ... 61
4.3.5 Ransomware ... 66
4.3.6 Zamjena SIM-a ... 68
4.3.7 Lažni novčanik ... 70
4.3.8 Napad na digitalnu vozačku dozvolu ... 74
5. Vrste rizika kod primjene tehnologije lanca blokova ... 79
5.1 Operativni i IT rizici ... 80
5.2 Rizici sigurnosti podatka ... 80
5.3 Regulatorni rizik ... 81
5.4 Rizik dobavljača trećih strana ... 81
5.5 Rizik privatnosti ... 82
6. Procjena rizika tehnologije lanca blokova ... 83
6.1 Čimbenici rizika ... 83
6.2 Model procjene i podaci o prijetnjama ... 84
6.2.1 Izvor prijetnji ... 84
6.2.2 Potencijalne prijetnje ... 85
6.2.3 Vjerojatnost prijetnje ... 85
6.2.4 Posljedice prijetnje ... 86
6.3 Rezultat procjene rizika ... 87
7. Tehnička analiza mobilne aplikacije lažni novčanik ... 94
7.1 Mobilne aplikacije „*Trezor Mobile Wallet*“, primjer prvi ... 94
7.2 Mobilne aplikacije „*Trezor Mobile Wallet*“, primjer drugi ... 98
8. Zaključak ... 103
9. Literatura ... 104

1. Uvod

Termin *blockchain* koji se svakodnevno koristi i u hrvatskom jeziku, jednostavno se može prevesti kao lanac blokova. Početak lanca blokova se obično računa od trenutka nastanka prve kriptovalute, bitcoina. No tvrdnja da je pojavom bitcoina prvi put primijenjena tehnologija lanca blokova nije u potpunosti točna. Naime, povijest lanca blokova je započela 1991. godine kada su kriptografi Stuart Haber i Scott Stornetta u dokumentu „*How to Time-Stamp a Digital Document*“ postavili temelje lanca blokova [1]. U dokumentu su autori opisali postupak kojim se vremenskim označavanjem digitalnog dokumenta postiže integritet i privatnost dokumenta.

Unatoč tome što je tehnologija lanca blokova prisutna više od 14 godina, smatra se relativno novom tehnologijom te jednim od najvažnijih izuma u posljednjih deset godina. Njezina popularnost svakim danom raste, najviše među inovatorima te pobornicima kriptovaluta. Primjena u području elektroničkog poslovanja je i danas zanemariva te se zbog toga još i danas često pojam lanac blokova veže uz kriptovalute. Tome je najviše pridonijelo nepovjerenje poslovnih subjekata prema novim tehnologijama, kao i strogi zakonodavni i regulatorni propis država koji su prilagođeni trenutnim poslovnim sustavima.

Tehnologija lanca blokova stoji iza kriptovaluta kao što su bitcoin, ethereum ili litecoin. Kada se govori o lancu blokova, navode se njegove prednosti poput decentralizacije, što znači da nije u vlasništvu jednog subjekta, i nepromjenjivost, budući da je nemoguće mijenjati podatke zapisane u bloku lanca blokova. Pohranjeni podaci i podaci koji se prenose su šifrirani, što praktički u potpunosti otklanja mogućnost za krivotvorenje ili dvostruko trošenje digitalne imovine. Tehnologija lanca blokova u poslovnim sustavima može donijeti velike uštede budući da protokol konsenzusa ulijeva pouzdanje u ispravnost svih podataka bez potrebe za posrednikom treće strane. Danas se tehnologija lanca blokova koristi za obavljanje brzih i sigurnih financijskih transakcija, a također se implementira u sustavima za praćenje roba i imovine, bolničkim sustavima i sustavima za digitalni identitet.

Unatoč mnogim prednostima tehnologije lanca blokova, ona također ima određene sigurnosne rizike. Napadači nastoje iskoristiti navedene rizike, a budući da se velika sredstva nalaze u lancu blokova, ekosustavi koji koriste lanac blokova su često meta napadača. Također, kako je tehnologija lanca blokova još uvijek u ranoj životnoj fazi, podložna je regulatornoj i

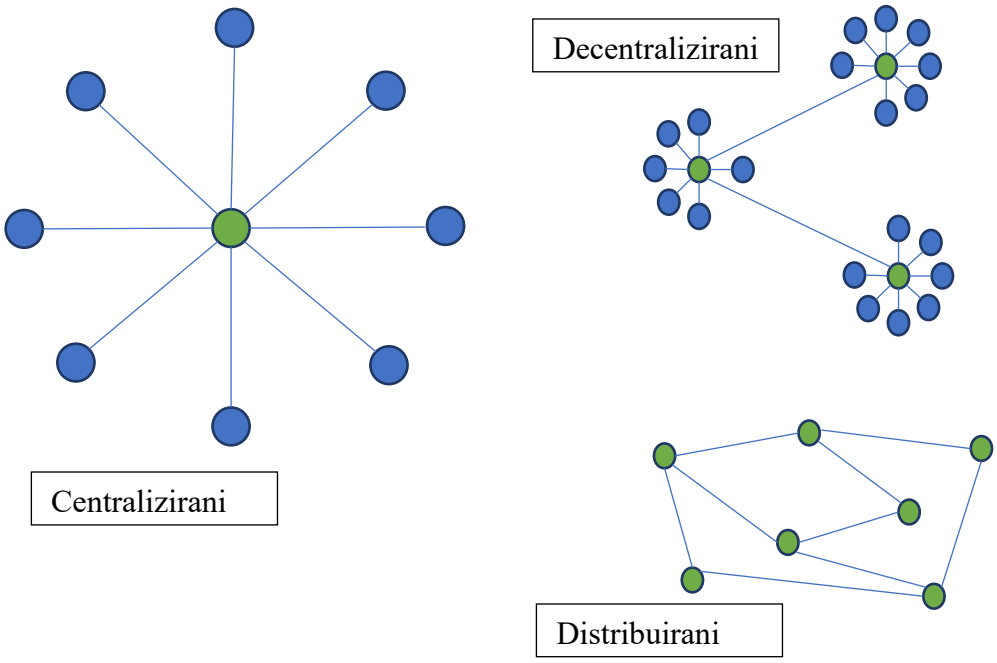
zakonodavnoj nesigurnosti. Stoga tvrtke i korisnici moraju biti svjesni mogućih rizika povezanih s korištenjem tehnologije lanca blokova.

U specijalističkom radu, tehnologija lanca blokova je promatrana sa sigurnosnog aspekta navodeći slabosti, ranjivosti i napade na sustave koji koriste tehnologiju lanca blokova.

U drugom poglavlju detaljno je opisana tehnologija lanca blokova, dok je u trećem poglavlju navedena primjena tehnologije lanca blokova u elektroničkom poslovanju. Četvrto poglavlje sadrži slabosti i ranjivosti lanca blokova uz primjere napada i studije slučajeva. U petom poglavlju su opisani rizici koji se nalaze u primjeni tehnologije lanca blokova. Šesto poglavlje sadrži procjenu rizika tehnologije lanca blokova uz prijetnje koji su temelji za spomenute napade u ovom radu. U sedmom poglavlju je napravljena tehnička analiza mobilne aplikacije lažnog novčanika koja se mogla naći u mobilnim trgovinama, a koju su napadači koristili kako bi mogli doći do sredstava koji se nalaze na digitalnom novčaniku korisnika.

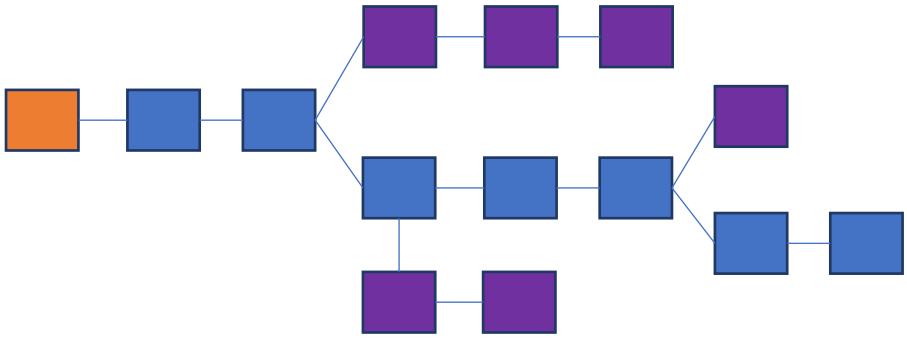
2. Tehnologija lanca blokova

Lanac blokova je struktura podataka koja se koristi za pohranu informacija u distribuiranim knjigama (eng. *distributed ledger*). U nekim literaturama se navodi da je lanac blokova decentralizirana baza podataka budući da se i lanac blokova i baza podataka koriste za pohranjivanje podataka. Lanac blokova čine zapisi, blokovi, koji su međusobno povezani sažetkom prethodnog bloka. Svaki blok sadrži podatke koji moraju biti potvrđeni da bi bili dodani u lanac blokova, sažetak prethodnog bloka, vremensku oznaku i podatke o transakciji. Lanac blokova je decentralizirani sustav (slika 2.1.) budući da ne postoji centralni poslužitelj koji upravlja i održava podatke, a promjene se ne mogu obaviti bez promjene svih prethodnih blokova u lancu, čime se osigurava integritet i sigurnost podataka. Decentralizacijom lanca blokova sustavi koji koriste tehnologiju lanca blokova izbjegavaju rizike neovlaštenog pristupa podacima i njezinog gubitka.



Slika 2.1. *Prikaz centraliziranog, decentraliziranog i distribuiranog sustava*

Lanac blokova se koristi u različitim poslovnim sustavima, uključujući financije, zdravstvo i trgovinu kao i u državnim uslugama kao što su upravljanje identitetom ili elektroničko glasovanje. Primjer korištenja lanca blokova između poslovnog subjekta i korisnika je korištenje tehnologije lanca blokova u svrhu osiguranja cjelovitosti i autentičnosti podataka u ugovorima, transakcijama, identitetima i drugim informacijama.



Slika 2.2. *Prikaz odlučujućeg lanca blokova (plavi) s alternativnim lancima (ljubičasti)*

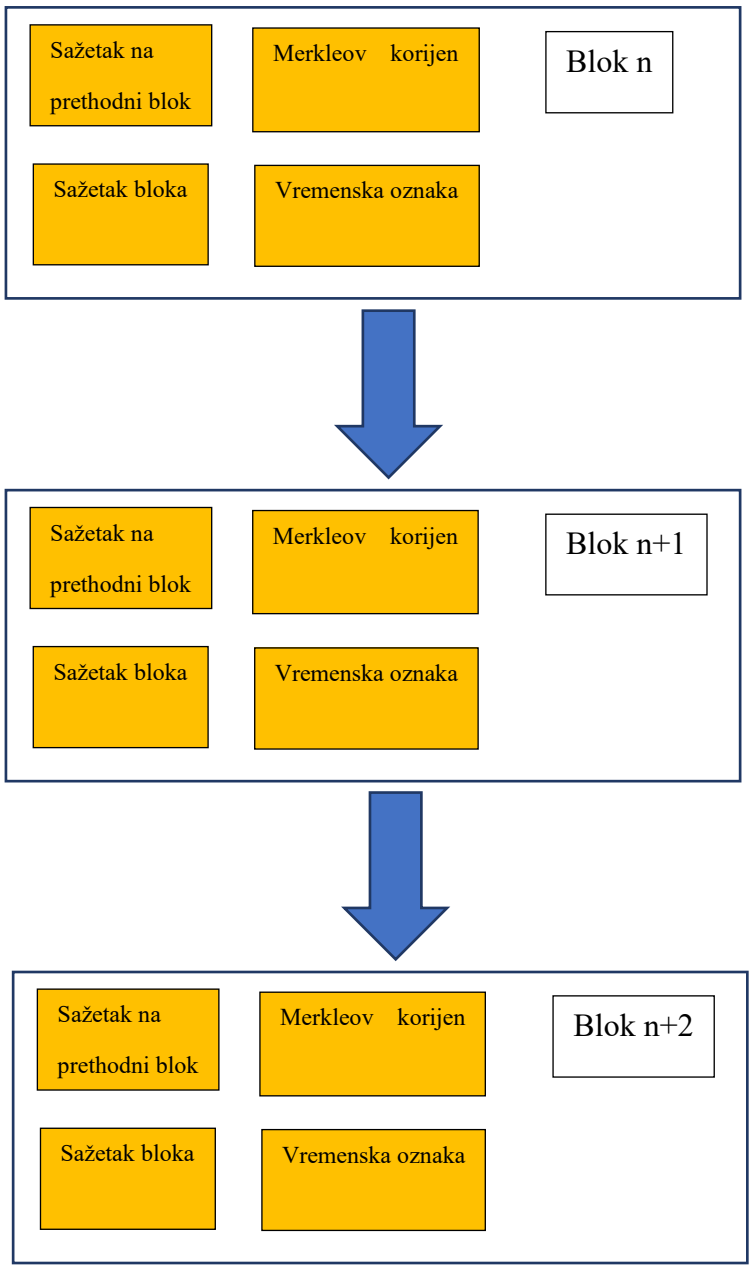
Na slici 2.2. se može vidjeti da se lanac blokova ne sastoji od jednog niza blokova, već je moguće grananje lanca. Odlučujući lanac (plavi) sastoji se od najdužeg niza blokova, dok alternativni lanci (ljubičasti) završavaju, čime su kraći od lanca nositelja.

Značajka tehnologije lanca blokova je disperzija moći među članovima mreže, čvorovima. Čvorovi su računala na kojima se nalazi klijent s kojim se povezuje na lanac blokova. Kopije lanca blokova se nalaze na svakom čvoru. Nakon što se potvrdi transakcija, dodaje se novi blok, nakon čega se lanac blokova na svim čvorovima ažurira. Čvorovi međusobno komuniciraju putem šifriranih poruka, a zapisi u blokovima su također šifrirani. Svaki čvor ima javni i privatni ključ. Javni ključ se koristi kod primanja sredstava i za identifikaciju korisnika, dok se privatni ključ koristi za pristup i kontrolu sredstava i čuva se tajnim. Svaki blok se pohranjuje na kraju lanca što u konačnici otežava promjenu sadržaja bloka. Sadržaj bloka se može promijeniti u slučaju da većina mreže postigne konsenzus o promjeni.

Ključni elementi lanca blokova su distribuirana knjiga, nepromjenjivi zapisi i pametni ugovori (eng. *Smart contracts*). Distribuirana knjiga sadrži evidenciju transakcija koje se bilježe samo jednom, čime se eliminira mogućnost dupliciranja koje je tipično za tradicionalne poslovne sustave. Svi sudionici mreže imaju pristup distribuiranoj knjizi i njenim transakcijama. Kada govorimo o nepromjenjivim zapisima u tehnologiji lanca blokova, misli se na nemogućnost mijenjanja ili brisanja bilo koje transakcije nakon evidentiranja u zajedničkoj knjizi od strane ni jednog sudionika mreže. Ako transakcija sadrži pogrešku, potrebno je dodati novu transakciju koja poništava pogrešku i tada su obje transakcije vidljive. Pametni ugovori služe kako bi se ubrzala transakcija. To je skup pravila koji su pohranjeni u lancu blokova i koji se primjenjuju i izvršavaju. Pametni ugovor može definirati uvjete za prodaju obveznica, uključiti uvjete za prodaju zdravstvenog osiguranja i slično.

Prednosti tehnologije lanca blokova su sljedeće [2]:

- Ušteda vremena – ne postoji centralno tijelo kroz koje je potrebno provesti sve transakcije. Proces obrade se umjesto u danima sada broji u minutima, a provjera transakcije sada se broji u satima.
- Manji troškovi – budući da svi sudionici dijele istu bazu, transakcije se obavljaju unutar distribuirane, dijeljene knjige čime se radi ušteda nad troškovima koji bi nastali u slučaju da svaki sudionik održava svoju bazu. Tradicionalni transakcijski sustavi zahtijevaju uključivanje treće strane radi kontrole transakcije uz plaćanje naknade.
- Sigurnost – sustav je siguran od kibernetičkih prijetnji budući da nitko ne može utjecati na podatke u lancu blokova koji su podijeljeni između čvorova. Nakon što član mreže potvrdi transakciju, ona se dodaje u blok lanca blokova. Svaki od blokova u lancu sadrži jedinstveni sažetak (eng. *hash*) zajedno s jedinstvenim sažetkom prethodnog bloka. U slučaju da se podaci sadržani u bloku uređuju na bilo koji način, sažetak bloka će se promijeniti, međutim sažetak u sljedećem bloku se neće mijenjati (slika 2.3.)
- Privatnost – svaki korisnik mreže može pristupiti povijesti transakcija, ali neće imati pristup informacijama koje identificiraju sudionike.
- Pouzdanost – lanac blokova certificira i provjerava identitet sudionika što uklanja potrebu za dvostrukom evidencijom te u konačnici ubrzava transakciju.



Slika 2.3. *Stvaranje i struktura bloka lanca blokova*

2.1 Protokoli i algoritmi lanca blokova

Najvažnije komponente lanca blokova su protokol i algoritam. Kada je bitcon 2009. godine predstavljen javnosti, pojavio se pojam protokol konsenzusa. Definicija algoritma je skup pravila ili procesa koje je potrebno slijediti u svrhu rješavanja nekog problema dok je

protokol definirana procedura ili sustav pravila koji omogućuje dijeljenje podataka između objekata na mreži.

Algoritam konsenzusa ima ključnu ulogu u određivanju dodavanja blokova u lancu i provjere valjanosti zapisa. To je algoritam koji čvorovima u mreži omogućuje postizanje dogovora o stanju mreže i izvornom stanju podataka, a čime se osigurava stabilnost i ispravnost mreže. U sustavima lanca blokova, algoritam konsenzusa se koristi za dijeljenje podatka između čvorova u mreži. Postoje mnogo različitih konsenzusnih algoritama, no dva su glavna oblika, dokaz o radu (eng. *Proof of work* - PoW) i dokaz o udjelu (eng. *Proof of stake* – PoS). Oba mehanizma se koriste u mrežama koje promjene usvajaju konsenzusom i koriste se prilikom obrade transakcije, potvrde informacija i u konačnici, u samoj sinkronizaciji podataka.

Važno je istaknuti da pored spomenuta dva vodeća algoritma postoji više od 30 konsenzusnih mehanizama koji se primjenjuju ili su još u razvojnoj fazi.

2.1.1 Dokaz o radu (PoW)

Kod klasičnog vida bankarstva dokaz o radu je potvrda banke, knjigovodstvenog servisa ili neke druge treće strane koja je provjerila ispravnost transakcije. Kod algoritma dokaz o radu, cilj svakog čvora je dobiti privilegiju, zadatak, da potvrdi zapis bloka. Zbog toga se čvorovi decentralizirane mreže međusobno natječu kako bi dobili tu privilegiju. Da bi potvrdili transakciju, čvor mora prvi uspješno riješiti zadatak postavljen od mreže. Zadatak čvorova je pronaći sažetak čija vrijednost je manja od vrijednosti ciljne težine. Ciljnu težinu računa mreža lanca blokova, a čvor koji prvi generira sažetak manje vrijednosti od vrijednosti ciljne težine je pobjednički čvor.

```
Ciljna težina =
000000000000003A30C0000000000000000000000000000000000000000
```

```
Pobjednički sažetak =
0000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569
```

Ciljna težina je promjenjiva vrijednost koja se prilagođava, ponovno računa, svakih 2016 blokova. Cilj je da utrošeno vrijeme potrebno za generiranje novog bloka bude približno 10 minuta. Iz toga proizlazi da je za generiranje 2016 blokova potrebno dva tjedna, što znači da se

nova ciljna težina računa svaka dva tjedna. Što je ciljna težina manja, veći je broj sažetaka koje čvor mora generirati da bi riješio zadatak, što u konačnici zahtjeva više računalnih resursa i veću potrošnju električne energije. Formula po kojoj mreža računa novu ciljnu težinu je

$$\Delta_1 = \frac{\Delta_0 * \mathrm{t}}{20160\ minuta}$$

Δ_1 – nova ciljna težina

Δ_0 – trenutna ciljna težina

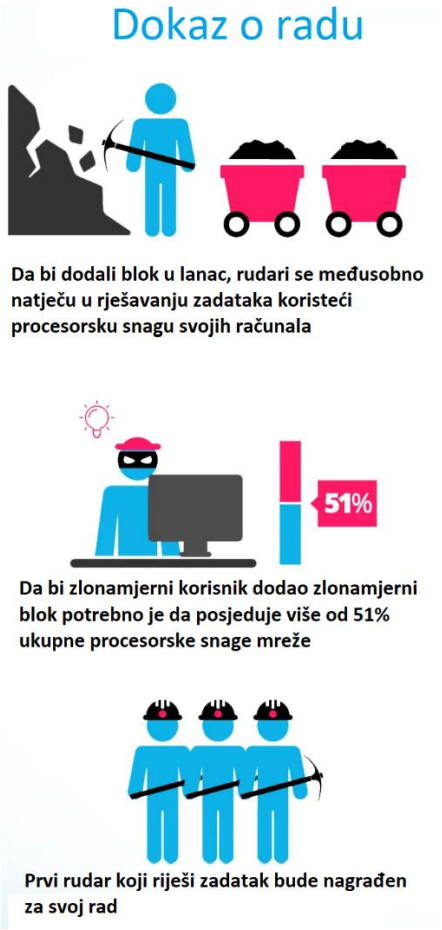
t – utrošeno vrijeme za generiranje posljednjih 2016 blokova

Ulazni podaci s kojima čvorovi generiraju sažetak, a koji se uspoređuje s ciljnom težinom, su verzija protokola, referenca na sažetak prethodnog bloka, sažetak korijena Merkleovog stabla transakcije bloka, vremenska oznaka, ciljna težina i jednokratni nasumični broj (eng. *nonce*). Kod bitcoina nasumični broj je cijeli broj u rasponu od 0 do 4 294 967 296 i jedini je ulazni podatak koji je čvorovima nepoznanica kod svake transakcije. Čvor da bi pronašao pobjednički, manji sažetak od ciljnog sažetka, mora nasumično pogađati jednokratni nasumični broj upotrebom grube sile i generirati milijune sažetaka u sekundi kako bi generirao pobjednički sažetak. Čvor koji pronađe nasumični broj s kojim se generira sažetak manji od sažetka ciljne težine može dodati novi blok u lanac blokova, a za što će zauzvrat biti nagrađen u vidu kovanica. Prije dodavanje novog bloka u lanac mreže, svaki čvor mreže radi provjeru ispravnosti novog bloka. Kako se novi blok širi mrežom, svaki čvor izvodi niz testova radi provjere ispravnosti bloka, a prije prosljeđivanja bloka sljedećem čvoru. Na ovaj način se osigurava da samo važeći blokovi se šire mrežom. Kada čvor primi novi blok, potvrdit će njegovu valjanost nakon provjere prema sljedećim kriterijima:

- Struktura bloka je važeća,
- Sažetak zaglavlja bloka manji je od ciljne težine,
- Provjerava vremensku oznaku bloka,
- Veličina bloka je unutar prihvatljivih granica.

Cilj mreže je da se u prosjeku svakih 10 minuta generira novi sažetak, a sam proces se naziva rudarenje. Sve transakcije se zapisuju kao blokovi u decentraliziranoj glavnoj knjizi.

Kako bi potencijalni napadač stekao mogućnost napada na mrežu, potrebno je da osigura računalne resurse, a samim time i veliku količinu energije kako bi izveo napad.



Slika 2.4. *Funkcioniranje koncepta dokaz o radu*

Dokaz o radu je prvi konsenzusni algoritam koji je predstavljen. Njegov veliki nedostatak je velika potrošnja energije koja se troši prilikom potvrde transakcije i izvođenja funkcije sažimanja. Kao odgovor na navedeni problem predložen je dokaz o udjelu, kao alternativni konsenzusni algoritam.

2.1.2 Dokaz o udjelu

Kao i u dokazu o radu, ispravnost transakcije provjerava nasumično odabran čvor, ali vjerojatnost dodjele mogućnosti validacije zapisa bloka se povećava s veličinom udjela, odnosno broja kovanica u vlasništvu čvora. Čvorovi koji potvrđuju transakciju se nazivaju

kovači i u većini slučajeva za validaciju dobivaju nagradu u vidu kovanica. Kako bi lanac blokova ostao siguran prilikom korištenja algoritma dokaza o udjelu, algoritam mora osigurati mehanizam kako bi se spriječilo zlonamjernog korisnika ili grupu korisnika od mogućnosti preuzimanja većine provjera ispravnosti transakcija. Način na koji to dokaz o udjelu postiže je zahtijevanje od kovača određene količine sredstava, kovanica, kako bi dobio privilegiju za potvrdom zapisa bloka. Time se od potencijalnog napadača zahtijeva veliki dio kovanica kako bi pokrenuo napad. Neki mehanizmi umjesto samog broja kovanica za definiranje uloge kovača koriste mehanizme kao što su „starost" kovanica, umnožak broja kovanica i vremena koje ih korisnik drži kod sebe.

Za algoritam dokaz o udjelu, budući da koristi sustav prema kojem favorizira korisnike s većem količinom kovanica, neki stručnjaci su smatrali da će dovesti do toga da sustav bude više centraliziran, prema čemu bi korisnici s velikom količinom kovanica imali veliki utjecaj na lanac blokova.

Slika 2.5. *Funkcioniranje koncepta dokaz o udjelu*

Prednost ovog algoritma, u odnosu na algoritam dokaz o radu, je i do tisuću puta manja potrošnja energije. U siječnju 2022., potpredsjednik Europske agencije za vrijednosne papire i tržišta, je pozvao Europsku uniju da zabrani model dokaz o radu u korist modela dokaza udjela zbog njegove manje potrošnje energije [3].

Tablica 2.1. *Usporedba dva vodeća konsenzusna algoritma*

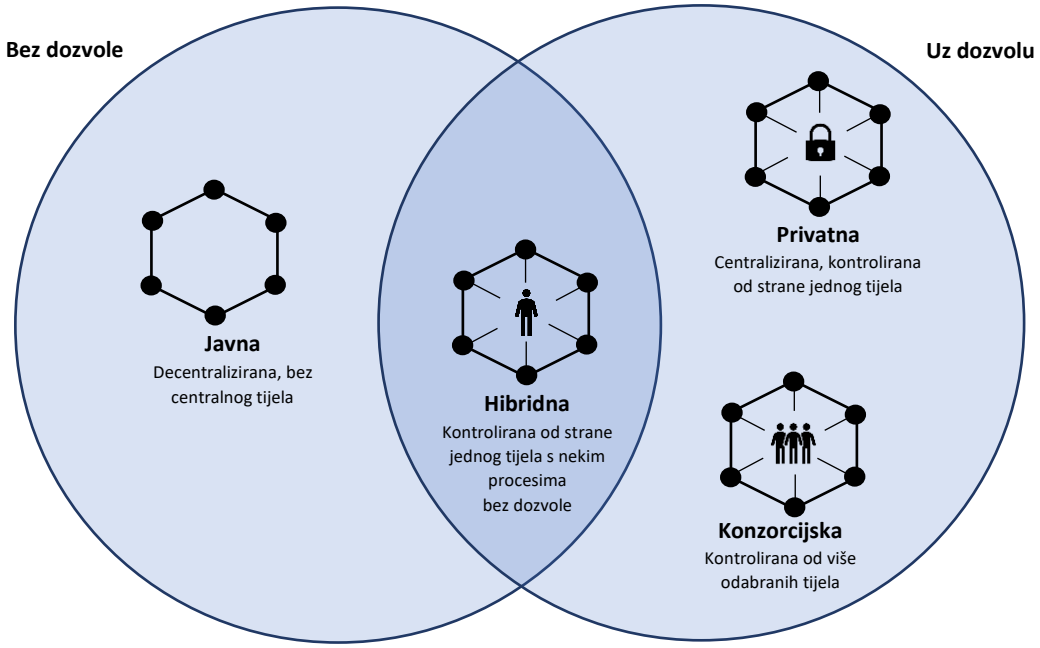
	Dokaz o radu (PoW)	Dokaz o udjelu (PoS)
Potvrda transakcije	• Čvorovi koji potvrđuju transakciju nazivaju se rudari. • Računalna snaga rudara je parametar za određivanje rudara za potvrdu transakcije.	• Čvorovi koji potvrđuju transakciju nazivaju se kovači. • Veličina uloga u sustavu je parametar za određivanje kovača.
Prednosti algoritma	• Visoka razina sigurnosti algoritma.	• Ne zahtijeva skupu opremu. • Veća skalabilnost.
Nedostaci algoritma	• Visoka potrošnja energije. • Zahtijeva skupu opremu, • Problem skalabilnosti.	• Bogati postaju bogatiji.
Primjer primjene	Bitcoin	Ethereum

2.2 Vrste tehnologije lanca blokova

Postoji nekoliko načina za izgradnju mreže lanca blokova (slika 2.6.).

a) javna mreža lanca blokova,
b) privatna mreža lanca blokova,
c) konzorcijski lanac blokova,

d) hibridni lanac blokova.



Slika 2.6. *Različite mreže lanca blokova*

U javnu mrežu bilo tko može pristupiti u svojstvu čvora kako bi sudjelovao u procesu potvrde transakcije te na taj način doprinijeti konsenzusu. Svaki sudionik može verificirati i potvrditi transakciju, a sve aktivnosti su transparentne i javno vidljive. Primjer javnog lanca blokova je Bitcoin. Javna mreža je decentralizirana, ali budući da je javna, mreža koristi dokaz o udjelu ili dokaz o radu kao konsenzusne algoritme, koji bi trebali spriječiti zlonamjerne korisnike od utjecaja na mrežu. U javnoj mreži se za sredstvo plaćanja naknade ili nagrade čvorovima prilikom potvrde transakcije koristi kriptovaluta. Sudjelovanje čvorova, radi postizanja konsenzusa, sustav čini sigurnijim, a kriptovalutu neophodnim sredstvom. Primjer korištenja javne mreže lanca blokova je glasovanje putem interneta.

Privatnoj mreži lanca blokova moguće je pristupiti samo uz odobrenje, a transakcije se ne mogu provjeravati u javnoj bazi. Privatna mreža je sustav kreiran za potrebe jedne organizacije, stoga se smatra centraliziranom mrežom. Zbog toga se u odnosu na javnu mrežu smatra manje sigurnom iz razloga što je ograničen na razini jedne organizacije. Prednost privatne mreže u odnosu na javnu je u brzini obrade transakcije koja je zbog veličine mreže brža u odnosu na

obradu transakcije u javnoj mreži. Primjer korištenja privatne mreže lanca blokova je upravljanje opskrbnim lancem poduzeća.

Konzorcijski lanac blokova je iz sustava izbacio kriptovalutu kao sredstvo za plaćanje naknade budući da svaki čvor mreže u konsenzusu djeluje u najboljoj namjeri i s istim ciljem. Nijednom sudioniku nije u interesu da svojom aktivnošću prouzroči nepovjerenje u tehnologiju čime ovi sustavi postaju samoodrživi i neovisni. Sudionicima konzorcijskog lanaca blokova moguće je pristupiti samo uz odobrenje, a sustav se u odnosu na javni i privatni lanac blokova smatra djelomično centraliziranim budući da više odabranih čvorova različitih organizacija sudjeluje u postizanju konsenzusa.

Hibridni lanac blokova koristi najbolje iz mreže lanca blokova bez dozvole i uz dozvolu kombinirajući značajke privatnih i javnih mreža lanca blokova. Omogućuje subjektima, tvrtkama, da izgrade privatni sustav temeljen na dozvolama uz javni sustav bez dozvola. U hibridnom lancu blokova transakcije i zapisi obično nisu javni, ali se mogu potvrditi, ako je potrebno, putem pametnih ugovora. Hibridni lanac blokova je, što se tiče sigurnosti, prilično siguran budući da djeluje unutar zatvorenog okruženja što je ujedno i nedostatak zbog netransparentnosti. Informacije se mogu sakriti, a korisnici mreže nemaju poticaja za sudjelovanjem u radu mreže. Hibridni lanac blokova može naći svoju primjenu u visoko reguliranim sustavima (npr. bankarskom sustavu) ili maloprodaji gdje može pomoći trgovcima da pojednostave svoje procese.

Tablica 2.2. *Usporedba karakteristika tehnologija lanca blokova*

	Javni	Privatni	Konzorcijski
Tip mreže	Decentralizirani	Centralizirani	Djelomično centralizirani
Pristup mreži	Svi	Unutar organizacije	Više odabranih organizacija
Čvorovi	Pristup bez dozvole, Nepoznat identitet	Pristup s dozvolom, Poznat identitet	Pristup s dozvolom, Poznat identitet
Sigurnost	Visoka PoW, PoS	Niska	Visoka
Postizanje konsenzusa	Rudari, Kovači	Unutar organizacije	Odabrani čvorovi u mreži
Brzina transakcije	Niska	Visoka	Visoka

2.3 Kriptografija u lancu blokova

Kriptografija, odnosno šifriranje, je jedna od metoda koja se koristi kod zaštite podataka u lancu blokova. Poruke koje se izmjenjuju između čvorova u lancu blokova šifriraju se primjenom asimetrične metode čime se štiti privatnost i integritet podataka. Pored šifriranja poruka između čvorova u mreži, lanac blokova sažima informacije prethodnog bloka i zapisuje ga u novi blok čime se osigurava cjelovitost lanca blokova i štiti lanac blokova od neovlaštene promijene podataka. Ako se bilo koja informacija iz bloka *n-1* promijeni, vrijednost zapisanog sažetka u bloku *n* će se također promijeniti što također mijenja vrijednost sažetka u bloku *n+1*.

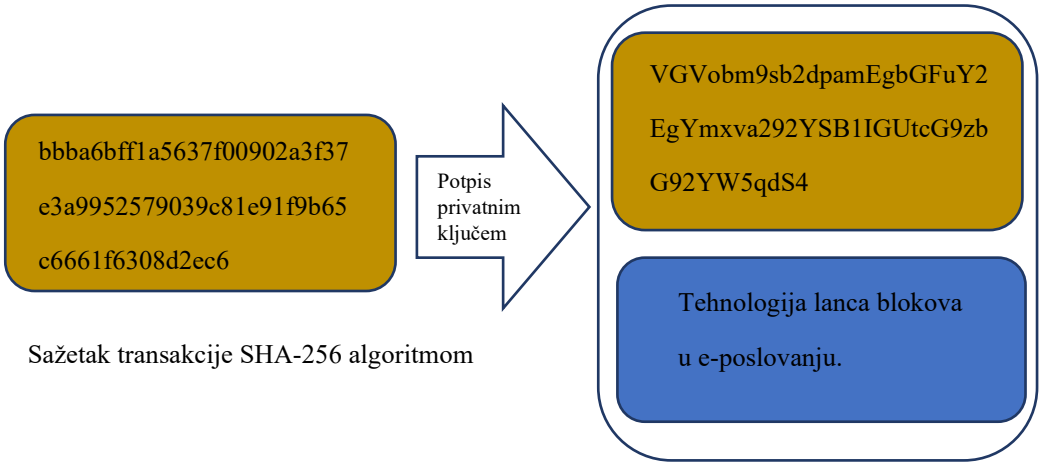
Lanac blokova sve transakcije šifrira primjenom asimetrične metode šifriranja, korištenjem parova javno-privatnih ključeva. Iz aspekta informacijske sigurnosti važno je slijediti stroga pravila i procedure prilikom upravljanja ključevima što uključuje ljude, procese i tehnologiju. Proces prijenosa sredstava između korisnika u lancu blokova uključuje identifikaciju korisnika, kreiranje i potpisivanje transakcije, provjera valjanosti transakcije od strane čvora na mreži i zapisivanje transakcije u lancu blokova. Koraci u prijenosu sredstava između računa su sljedeći:

1. Identifikacija korisnika - javni ključ se koristi za identifikaciju korisnika te kao adresa za primanje sredstava, novčanik.
2. Kreiranje transakcije - korisnik koji želi prenijeti sredstava kreira transakciju. Transakcija sadrži informacije o primatelju i iznosu koji se šalje.
3. Potpisivanje transakcije - pošiljatelj svojim privatnim ključem potpisuje transakciju čime se potvrđuje da je transakciju izvršio vlasnik adrese, odnosno novčanika.
4. Slanje transakcije - potpisana transakcija se šalje u mrežu radi provjere valjanosti.
5. Uključenje u blok - nakon uspješne provjere transakcije, čeka se na uključenje transakcije u novi blok.
6. Potvrda transakcije - nakon što je transakcija uspješno uključena u blok, transakcija je potvrđena.
7. Ažuriranje stanja na računu - nakon potvrde transakcije, stanje računa primatelja i pošiljatelja se ažuriraju.

Čvor koji provjerava transakciju naziva se rudar ili kovač, ovisno o protokolu koji mreža koristi. Ukoliko se poruka nakon potpisivanja transakcije izmijeni, transakcija se odbija.

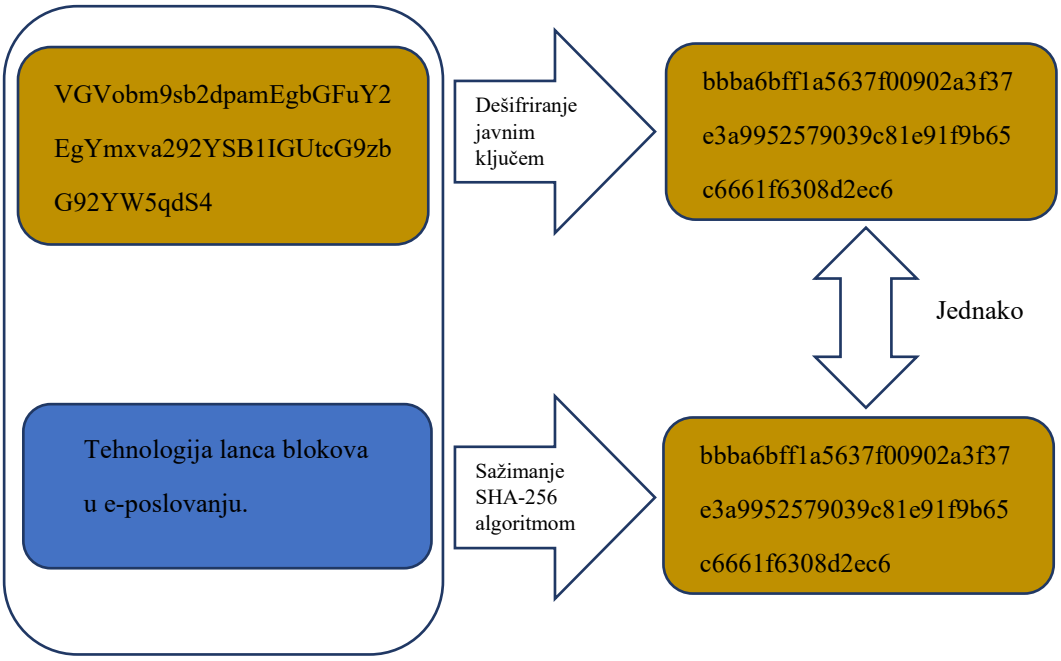
Jedna od obećavajućih primjena lanaca blokova je korištenje pametnih ugovora u lancu blokova. Pametni ugovori su digitalni ugovori pohranjeni u lancu blokova koji se automatski izvršavaju kada se ispune određeni uvjeti [4]. Izvršavaju se automatski, bez uključivanja trećih strana, uz uštedu vremena. Tijek izvršavanja može se automatizirati do te mjere da izvršavanje pametnih ugovora, nakon što se ispune uvjeti, može pokrenuti sljedeći proces.

Kako bi čvor dokazao svoju legitimnost u mreži lanca blokova, a čime stječe pravo obavljanja transakcija, potrebno je da čvor kreira jedinstveni digitalni potpis. Prije nego čvor potpiše transakciju privatnim ključem, originalna transakcija se sažima korištenjem SHA-256 algoritma (slika 2.7.). Digitalnim potpisivanjem sažetka transakcije sačuvali smo integritet i neporecivost transakcije, a slanjem javnog ključa zajedno sa transakcijom osigurana je autentičnost poruke.



Slika 2.7. *Kreiranje digitalno potpisane transakcije*

Potpisana transakcija i javni ključ pošiljatelja se šalju u mrežu lanca blokova radi provjere ispravnosti transakcije od strane sudionika u mreži. Nakon što svi čvorovi prime digitalno potpisanu transakciju, konsenzusnim algoritmom se određuje koji će čvor dobiti privilegiju da verificira transakciju, stvoriti novi blok i dodati ga u lanac blokova. Odabrani čvor izračunava vrijednost sažetka transakcije i uspoređuje ga s dešifriranom vrijednošću sažetka reference na transakciju koju je dešifrirao pomoću javnog ključa pošiljatelja. Ukoliko su oba sažetka jednaka, transakcija je ovjerena čime se dodaje novi blok u lanac blokova (slika 2.8.).

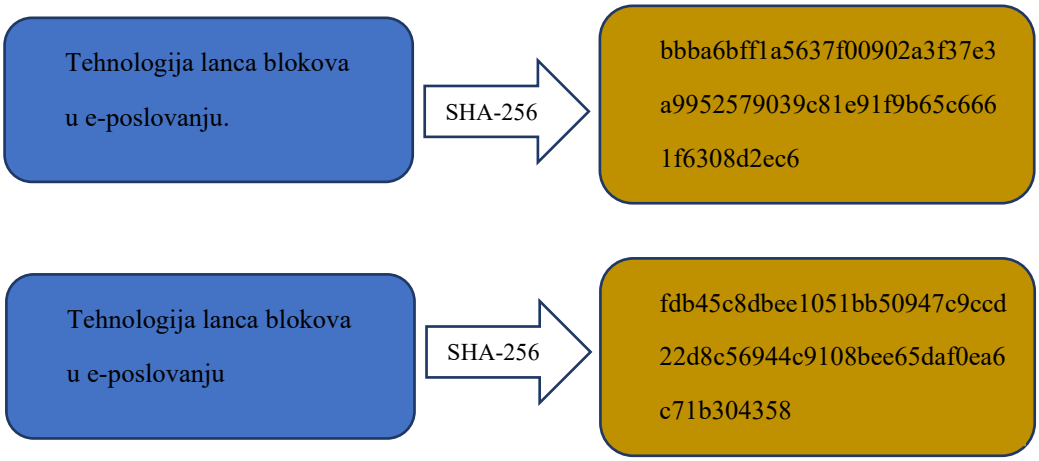


Slika 2.8. *Verifikacija transakcije*

2.3.1 Sažimanje

Kao što je već spomenuto u prethodnom poglavlja, prilikom kreiranja novih blokova koristi se funkcija sažimanja koja iz dva ulazna podataka, a koji teoretski mogu biti beskonačne veličine, generira zapis fiksne veličine. Sažimanje omogućava nepromjenjivost u lancu blokova, a funkcija sažimanja ne uključuje upotrebu ključeva. Kada je transakcija potvrđena, algoritam kreira novi blok koji čini vremenska oznaka, sažetak, sažetak na prethodni blok i podatke o transakciji. Funkcija sažimanja pomaže u povezivanju blokova i održavanju cjelovitosti podatka unutar bloka, a svaka izmjena u podacima bloka dovodi do prekida lanca blokova. Funkcija sažimanja mora ispuniti sljedeća svojstva:

- Jednostavnost izračuna – sažimanje je uz pomoć računala lako i brzo izračunati, a generirani zapis je fiksne veličine.
- Jednosmjerna operacija – iz generiranog zapisa nije moguće izračunati ulazni podatak.
- Determinističnost – izvršavanje funkcije sažimanja nad jednakim ulaznim podacima mora uvijek generirati jednak izlazni zapis.
- Otpornost na kolizije – izvršavanje funkcije sažimanja nad dva slična ulazna podatka nikad ne bi smjela generirati jednake izlazne zapise (slika 2.9.).



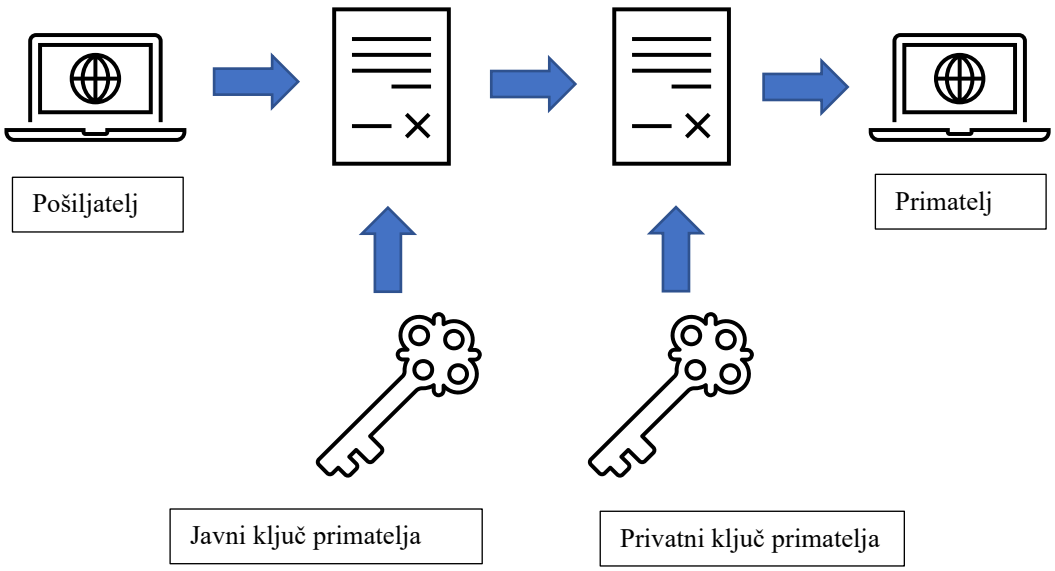
Slika 2.9. *Rezultat sažimanja sličnih poruka. Prva poruka sadrži točku na kraju dok je druga bez točke*

Prednosti korištenja funkcije sažimanja u lancu blokova:

- sprječavanje izmjena podataka u bloku
- lakša provjera transakcije
- transakcija zahtijeva manju propusnost.

2.3.2 Asimetrično šifriranje

Lanac blokova koristi asimetričnu metodu šifriranja čiji ključni elementi su javni i privatni ključ. Asimetričnim šifriranjem se daje mogućnost nepoznatim sudionicima da međusobno dijele informacije i može se koristiti na dva načina. Prvi način na koji se mogu koristiti ključevi je slučaj u kojem želimo primiti šifriranu poruku koju samo mi možemo dešifrirati. U tom slučaju, pošiljatelj šifrira poruku našim javnim ključem, a budući da je za šifriranje korišten naš javni ključ, poruka se može dešifrirati isključivo našim privatnim ključem (slika 2.10.).



Slika 2.10. *Asimetrično šifriranje kod slučaja šifriranja poruke javnim ključem primatelja*

Drugi slučaj upotrebe ključeva je kada želimo garantirati da je poruka poslana od nas. U tom slučaju poruka se potpisuje našim privatnim ključem, a primatelj za dešifriranje poruke koristi naš javni ključ. Ovaj slučaj asimetričnog šifriranja se primjenjuje u lancu blokova. Asimetrično šifriranje u lancu blokova ima svoju primjenu iz jednostavnog razloga, velikog broja korisnika. Asimetrično šifriranje je prikladno u višekorisničkom okruženju usmjerenom na pružanje povjerljivosti, a koristi se za digitalni potpis i distribuciju ključeva.

Lanac blokova je distribuirana i decentralizirana mreža. Svi sudionici u mreži, čvorovi, imaju odgovornost za održavanje vlastite kopije distribuirane knjige. Također lanac blokova omogućuje prijenos podataka u obliku blokova i transakcija između čvorova putem točka prema točki (eng. *peer-to-peer*) mreže. Prednosti korištenja asimetričnog šifriranje u lancu blokova su:

- Sigurnost podataka – bolja zaštita podataka u odnosu na metodu simetričnog šifriranja,
- Sigurnost privatnog ključa – privatni ključ je poznat samo vlasniku i ne zahtijeva prijenos privatnog ključa putem mreže čime se smanjuje mogućnost njegovog otkrivanja od strane zlonamjernih korisnika,
- Neporecivost transakcije – svaki korisnik ima odgovornost zaštite svojeg privatnog ključa.

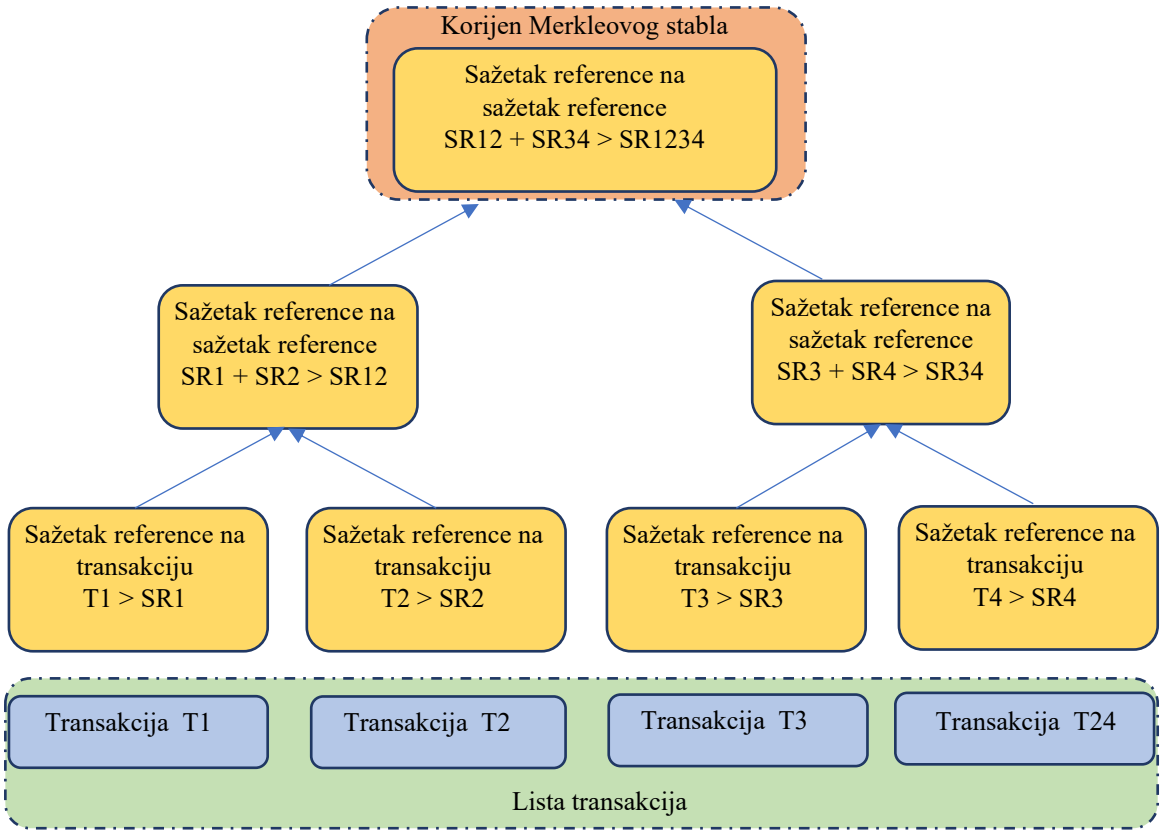
S druge strane, postoje i implikacije na lanac blokova i šifriranje asimetričnim ključem. Algoritmi asimetričnog šifriranje razvijaju parove ključeva koji su matematički međusobno povezani. Veličina duljine ključa uvelike utječe na ispunjavanje sigurnosnih zahtjeva i zahtijeva duljinu ključeva obično u rasponu od 2048 do 4096 bita. Time se uvelike usporava proces dešifriranja i u konačnici usporava brzina izvođenja transakcije. Velika količina podataka koja se nalazi na mreži je također jedan od parametara koji usporava algoritam šifriranja, što predstavlja još jedan vid ograničenja rada s asimetričnim šifriranjem. Vrijedi spomenuti i trenutni razvoj kvantnih računala što će u budućnosti omogućiti „razbijanje“ ključeva generiranih asimetričnim algoritmom u nekom razumnom vremenu. Također, uspjeh asimetričnog šifriranje uvelike ovisi o sposobnosti čuvanja privatnog ključa. Gubitkom privatnog ključa, ili njegovom krađom, gubi se pristup šifriranim podacima. Kao što je već spomenuto, privatni ključevi su poznati samo vlasniku čime sami postaju ciljevi zlonamjernih napadača.

2.3.3 Merkleovo stablo

Temeljna sastavnica lanca blokova je Merkleovo stablo. Merkleovo stablo je strojno strukturirana datoteka koja se koristi za potvrdu autentičnosti drugih podataka, a nazvano je po američkom inženjeru i znanstveniku, Ralphu Merkleu. U osnovi, to je lanac digitalnih potpisa koji omogućava da se provjeri ispravnost podataka unutar lanca blokova. Stablo pruža mogućnost brze provjere integriteta podataka i efikasno upravljanje velikim brojem transakcija. Kada se novi blok dodaje u lanac, sažetak prethodnog bloka se dodaje novom bloku kao sigurnosna potvrda da je prethodni blok ispravan. Ovaj postupak se nastavlja sa svakim novim blokom u lancu blokova što stvara lanac digitalnih potpisa koji se naziva Merkleovo stablo. Pored verifikacije podataka u distribuiranoj knjizi, Merkleovo stablo se koristi za sigurnu pohranu podataka [6].

Postupak kreiranja Merkleovog stabla prikazan je na slici 2.11. koja prikazuje nastanak stabla na primjeru četiri transakcije. Svaka se transakcija pojedinačno sažima korištenjem SHA-256 algoritma. Rezultat sažimanja transakcije je sažetak referenca na transakciju koji se nazivaju „listovi“. Na slici vidimo da je sažetak referenca transakcije 1 SR1. Susjedni sažetak reference podređenih čvorova spojen je u niz, a iz nastalog niza se izračunava sažetak reference na sažetak reference. Na slici je to prikazano spajanjem sažetka reference (SR3 + SR4) u sažetak referencu

SR34. Novonastali sažeti reference se ujedno nazivaju „granama“ i u Merkleovom stablu mogu predstavljati podređeni ili roditeljski čvor. Ovaj postupak se izvršava sve dok se ne izračuna posljednji sažetak. Posljednji sažetak se naziva korijen Merkleovog stabla (SR12 + SR34 > SR1234) i predstavlja nadređeni čvor.



Slika 2.11. *Kreiranje Merkleovog stabla*

2.4 Privatnost, sigurnost i povjerenje u lancu blokova

Lanac blokova, uz pomoću asimetričnog šifriranja i sažimanja, šifrira informacije koje se nalaze u blokovima čime osigurava privatnost podatka. Šifriranje se koristi i kod potvrde identiteta i autentičnosti transakcije što tehnologiji lanca blokova ujedno daje robusnost u zaštiti privatnosti. Privatnost je ono što je potaklo veliku rasprostranjenost korištenja kriptovaluta među kriminalcima koristeći kriptovalutu za kupovinu ilegalnih artikala i plaćanje kriminalnih usluga. Pojedine države koje se nalaze pod međunarodnim sankcijama su također koristile kriptovalute za zaobilaženje nametnutih sankcija. Primjer je DR Sjeverna Koreja koja je

koristila prednosti korištenja tehnologije lanca blokova i u kriptovaluti financirala svoj raketni program. Izvješće tvrtke za analizu lanca blokova „*Chainalysis*“ iz siječnja 2022. navodi da je Sjeverna Koreja tijekom 2021. ukrale gotovo 400 milijuna dolara u kriptovaluti [7].

Tehnologija lanca blokova je otklonila centralizaciju, koja predstavlja prijetnju u tipičnim sustavima za pohranu podataka. Decentralizacija lanca blokova je otklonila koncentraciju ranjivosti u jednoj točki. Decentralizacija također daje mogućnost zlonamjernim korisnicima anonimni napad na sustav.

Tehnologija lanca blokova je otklonila potrebu za povjerenjem u središnje tijelo. U primjeru financijske transakcije, kada korisnik šalje novac drugom korisniku, oba korisnika moraju imati povjerenje u treću stranu u obavljanju transakcije.

Mnogo je različitih primjera primjene tehnologije lanca blokova u različitim poslovnim sustavima. Ako uzmemo primjer u primjeni tehnologije lanca blokova u sustavu zdravstava, zdravstveni kartoni sadrže mnoge privatne i osjetljive podatke kao što su broj zdravstvenog osiguranja, OIB, kućna adresa pa i povijest bolesti. Ima primjera kada je zaštita ovih podataka na centralnom mjestu, koristeći centralizirani sustav pohrane, bila kompromitirana. Korištenjem lanca blokova i spremanjem zdravstvenih kartona isključivo u elektroničkom kartonu, omogućilo bi samim pacijentima da kontroliraju pristup svojim zdravstvenim kartonima putem privatnih i javnih ključeva. Transakcije bi imale vremensku oznaku čime bi se postigao kontrolirani pristup ažuriranim informacijama.

2.4.1 Pametni ugovor

Nekoliko puta je spomenuto da je izbjegavanje trećih osoba jedna od ključnih prednosti transakcija korištenjem tehnologije lanca blokova. Jedan od najvažnijih elemenata tehnologije lanca blokova je mogućnost korištenja pametnih ugovora (eng. *Smart Contract*). Korištenjem pametnih ugovora čvorovi automatski izvršavaju uvjete ugovora ako su prethodno ispunjeni svi uvjeti navedeni u ugovoru. Pametni ugovor nije ništa drugo nego ugovor upisan u obliku programskog koda u lanac blokova između dviju ili više strana. Budući da su podaci upisani u lanac blokova, to nam jamči integritet podataka. Ovime se otklanja potreba za sudjelovanjem treće strane koja je kod tradicionalnih ugovora potrebna kako bi napisala, odobrila ili nadgledala

ugovor. U tablici 2.3. navedene su razlike između pametnih ugovora i tradicionalnih ugovora [8].

Tablica 2.3. *Razlike između pametnih ugovora i tradicionalnih ugovora*

Pametni ugovori	Tradicionalni ugovori
Za izvršenje je potrebno nekoliko minuta	Za izvršenje je potrebno i do nekoliko dana
Bez sudjelovanja treće strane	Potrebno sudjelovanje treće strane (javni bilježnik, odvjetnik, banka)
Proces je digitaliziran	Proces nije u potpunosti digitaliziran i potrebna je fizička prisutnost
Troškovi procesa su minimalni	Troškovi procesa mogu biti značajni

Postoji nekoliko razloga primjene pametnih ugovora:

- Brzina provedbe – ispunjavanjem uvjeta iz ugovora, provedba ugovora se izvršava u svega nekoliko minuta.
- Sigurnost – uvjeti ugovora na lancu blokova se ne mogu samostalno mijenjati. Izvršene transakcije su zapisani u prethodnom bloku što bi u slučaju zlonamjerne izmjene zahtijevalo od napadača promjenu cijelog lanca blokova kako bi promijenio jednu transakciju.
- Povjerenje – svi uvjeti ugovora su šifrirani u lancu blokova, vidljivi su samo ugovornim stranama te naknadna izmjena definiranih stavki za obavljenu transakciju, a nakon provedbe ugovora, nije moguća.
- Ušteda – ostvaruje se velika ušteda u vidu financijske uštede i ušteda na vremenu izvršenja. Nije potrebno sudjelovanje trećih strana kao što su banke, javni bilježnici ili odvjetnici što iziskuje financijske izdatke.

Pametni ugovori će postati naša svakodnevnica kao što su danas tradicionalni ugovori.

Praktična primjena pametnih ugovora u elektroničkom poslovanju:

- Ugovaranje leasinga za kupnju radnog stroja – u slučaju da korisnik ne plati ugovorenu mjesečnu ratu, automatski se blokira mogućnost korištenja stroja.
- Ugovor o zakupu – u slučaju da korisnik poslovnog prostora ne plati ugovorenu mjesečnu zakupninu do dogovorenog datuma, ulazna vrata se zaključavaju.

- Internet trgovina – nakon što je roba naručena, uplata se zabilježi u lanac blokova. Nakon što dostavna služba potvrdi da je roba isporučena, i kupac potvrdi da je zadovoljan kvalitetom isporučene robe, novac se isplaćuje trgovcu. Ovo je primjer ugovora u kojem sudjeluju tri strane, trgovac, dostavna služba i kupac.

Svi ekosustavi koje koristi lanac blokova imaju implementirane pametne ugovore radi implementiranja logike izvršenja transakcije. Ako uzmemo primjer kriptovalute, ugrađeni pametni ugovori provjeravaju transakciju prilikom ulaza provjerom potpisa, zatim provjeravaju podatke o sudionicima transakcije nakon čega izvršavaju promjenu stanja na računima. Kako je opisao Nick Szabo, možda je najbolja metafora za pametni ugovor automat za prodaju grickalica [9]. S pravim unosom zajamčen je određeni izlaz.

```
Novac + odabir grickalica = užina podijeljena
```

U nastavku je prikazan programski kod pametnog ugovor napisan u Solidityju na primjeru kupnje na automatu za prodaju grickalica.

```
pragma solidity 0.8.7;

contract AutomatGrickalice {

    // Deklariranje varijable stanja ugovora
    address public owner;
    mapping (address => uint) public snackBalances;

    // Kada je ugovor 'AutomatGrickalice' implementiran:
    // 1. postavlja se adresa vlasnika ugovora
    // 2. postavlja se saldo pametnog ugovora za grickalice na
100
    constructor() {
        owner = msg.sender;
        snackBalances[address(this)] = 100;
    }
```

```
    // Dozvola vlasniku da poveća saldo pametnog ugovora
    function refill(uint amount) public {
        require(msg.sender == owner, "Samo vlasnik može
povećati saldo.");
        snackBalances[address(this)] += amount;
    }

    // Dozvola svima da mogu kupiti
    function purchase(uint amount) public payable {
        require(msg.value >= amount * 1 ether, "Minimalna
cijena je 1 ETH za grickalice");
        require(snackBalances[address(this)] >= amount, "Nema
grickalica na stanju");
        snackBalances[address(this)] -= amount;
        snackBalances[msg.sender] += amount;
    }
}
```

2.4.2 Lanac blokova i zakoni

Prema Općoj uredbi o zaštiti podataka u EU, osobni podaci su podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi [10]. Osobne podatke uključuju informacije kao što su [10]:

- ime i prezime,
- adresa,
- broj osobne iskaznice ili putovnice,
- primanja,
- kulturni profil,
- IP adresa,

- podaci u posjedu zdravstvene institucije.

GDPR se temelji na pretpostavci da u sustavu koji koristi osobne podatke postoji voditelj obrade podataka kojoj se pojedinac može obratiti kako bi ostvario prava zajamčena prema zakonima EU o zaštiti podataka. Problem primjene ove regulative kod korištenja tehnologije lanca blokova, administrativno gledajući, leži u nastojanju tehnologije lanca blokova u decentralizaciji. Zatim, problem u primjeni GDPR-a u lancu blokova je u nemogućnosti brisanja ili promjene podataka na zahtjev pojedinaca. Naime, prema zakonima GDPR-a, pojedinac ima pravo na zaborav ili brisanje podataka povezanim s njim. Budući da je lanac blokova nepromjenjiv, nemoguće je izbrisati podatke. Arhitektura distribuirane knjige, koja se koristi u lancu blokova, su baze podataka samo za dodavanje koje kontinuirano rastu kako se dodaju novi podaci te se ujedno zapisuju na mnogo različitih računala. Oba aspekta su problematična iz perspektive minimiziranja podataka. Naime, GDPR koristi načelo minimiziranja podataka i ograničavanja primjene istih prema kojem se podaci koji se prikupljaju moraju svesti na minimum i obrađivati samo u svrhe koje su unaprijed definirane. O svemu ovome moraju voditi računa arhitekti programskih rješenja temeljenim na tehnologiji lanca blokova.

Drugi problem je nemogućnost nadzora prihoda ostvarenim trgovinom kriptovalutama, a koje koriste tehnologiju lanca blokova, od strane poreznih i sudskih vlasti. Spomenuto je da je korištenje kriptovaluta od strane kriminalaca u kriminalne svrhe, pa čak i od strane vlada u svrhu izbjegavanja međunarodnih sankcija, doprinijelo masovnom korištenju kriptovaluta. Nemogućnost praćenja tijeka transakcija i povezivanja transakcija s pojedincem se koristilo u svrhu pranja novca i prikrivanja podrijetla novca. Mnogi pojedinci su trgovanjem kriptovalutama ostvarili zaradu koju nisu prijavili poreznoj upravi. Zbog sve učestalijeg investiranja u kriptovalute, porezna uprava SAD-a ovaj vid investicije tretira kao investiciju u dionice zbog čega podliježu novčanim kaznama u slučaju da ne prijave prihod od kriptovalute. Zbog toga je porezna uprava pozvala *Coinbase* da prijavi korisnike koji su poslali ili primili kriptovalute u vrijednosti većoj od 20.000,00 USD u godini [11]. *Coinbase* je američka tvrtka koja upravlja platformom za razmjenu kriptovaluta i po obujmu trgovanja to je najveća mjenjačnica kriptovaluta u SAD-u [12]. Na temelju sudske odluke iz studenog 2017., *Coinbase* je dostavio korisničke podatke (uključujući ime i prezime, broj socijalnog osiguranja, datum rođenja i aktivnosti na računu) poreznoj upravi za 14000 korisnika koji su napravili 20.000 USD prometa po svojim računima u jednoj godini [11]. Budući da je lanac blokova

decentraliziran, vlastima je teže pratiti transakcije i u konačnici kriptovalute čine pogodnim za pranje novca.

Prema „Smjernicama Savezne komisije za trgovinu SAD-a“ tehnologija lanca blokova je priznata kao tehnologija koja zadovoljava načelo o poštenoj informacijskoj praksi. To načelo predstavlja skup praksi o privatnosti i sigurnosti korisnika u elektroničkom poslovanju [13]. Tehnologija lanca blokova omogućava korisnicima kontrolu svojih podataka putem privatnog i javnog ključa, a trećim stranama nije dopušten pristup podacima bez dozvole i njihova zlouporaba.

3. Primjena lanca blokova u e-poslovanju

Trenutačni sustav e-poslovanja zahtijeva sudjelovanje treće osobe prilikom obavljanja transakcije. Ako uzmemo primjer e-trgovinu, pored kupca i trgovca, sustav plaćanja u e-trgovini uključuje i banku koja obavlja transakciju između kupca i trgovca. Sudjelovanje banke u e-trgovini ima svoj trošak u vidu bankarske naknade za obavljenu transakciju. Taj trošak se u vidu naknada naplaćuje od trgovca, ali isto tako trgovac taj trošak kroz svoju maržu prebacuje na kupca. Zauzvrat banka trgovcu jamči naplatu, dok ista banka prema kupcu ne daje nikakva jamstva za kupljeni proizvod osim jamstva sigurne kupnje. Kupac je zaštićen samo u slučaju da država ima donesen zakon o zaštiti potrošača i u slučaju da je transakcija obavljena unutar iste države ili zajedničkog tržišta (npr. primjer zajedničkog tržišta Europske unije). Ako na ovome primjeru izbacimo banku kao trgovca i transakciju obavimo putem mreže lanca blokova, smanjili bi se troškovi transakcije, a transakcija bi se mogla obaviti samo u slučaju da istu potvrde svi sudionici u poslovnom procesu.

Primjena tehnologije lanca blokova u e-poslovanju je još u povojima iako sigurnost samog sustava nadmašuje tradicionalni centralizirani sustav. Trenutno su male šanse za potpunu zamjenu tradicionalnog vida poslovanja, ali primjena tehnologije lanca blokova u pojedinim poslovnim procesima je put koji vodi ka potpunoj implementaciji u budućnosti.

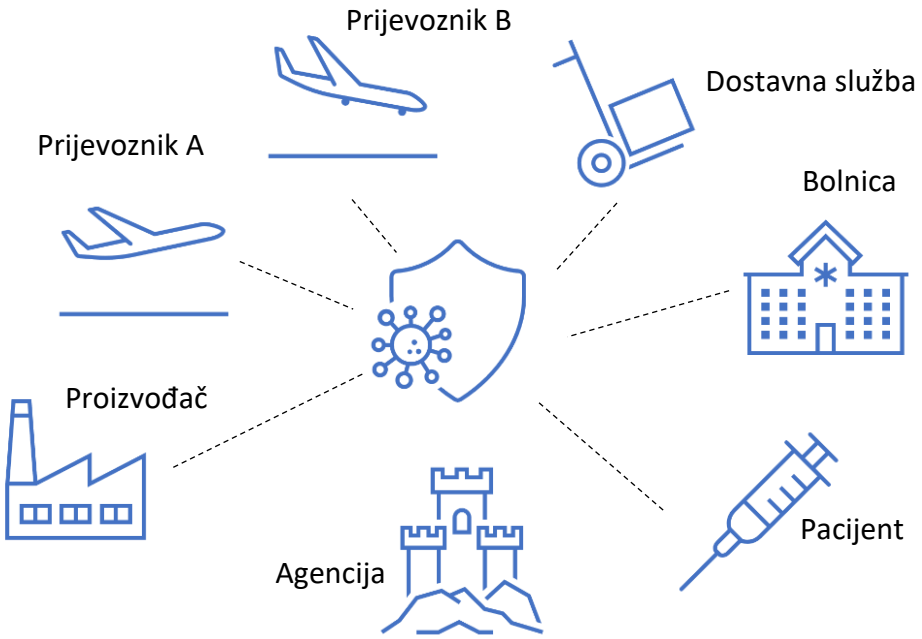
3.1 Lanac blokova i kriptovalute

Mnogi danas lanac blokova poistovjećuju s kriptovalutama, ali treba znati da je lanac blokova tehnologija koja se primjenjuje kako bi kriptovaluta uopće mogla funkcionirati. Lanac blokova je temelj kriptovalute. Kriptovaluta je virtualna valuta koju za razliku od konvencionalnih valuta, tzv. fiat valuta, ne izdaju središnje institucije, a stabilnost se održava pomoću složenih algoritama protokola. Zamjena kriptovalute u konvencionalnu valutu se odvija putem mjenjačnica. Tečaj u mjenjačnicama se formira ovisno o ponudi i potražnji za određenom kriptovalutom. Na dan 3. siječnja 2023. na tržištu se nalazi 22.174 kriptovalute s ukupnom kapitalizacijom od 761.987.436.030 EUR. Najdominantnije kriptovalute su bitcoin s udjelom od 39,8% u ukupnom udjelu kriptovaluta i ethereum s udjelom od 18,4% u ukupnom

udjelu [14]. Iz navedenog možemo vidjeti da prema udjelu bitcoina prevladava konsenzusni protokol dokaz u radu u odnosu na protokol dokaz u udjelu.

3.2 Lanac blokova i e-uprava

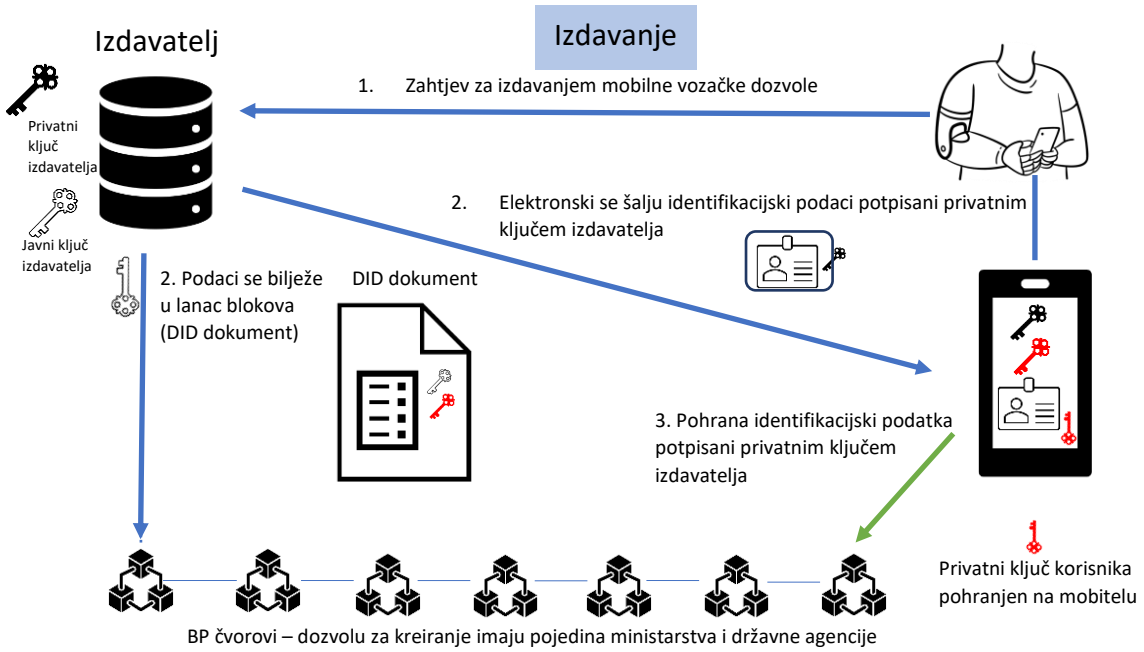
Da bi tehnologiju lanca blokova mogli jednostavno predočiti, uzet ćemo primjer servisa Googleov dokument. Lanac blokova možemo zamisliti kao snažno šifriran i verificiran dijeljeni Googleov dokument gdje svaki unos u listu ovisi o logičnom odnosu s prethodnim unosom, a s njime se slažu svi koji dijele dokument. Potencijal korištenja tehnologije je mnogo veći od trenutne implementacije u svijetu kriptovalute. Jedan od potencijala je vođenje evidencije pojedinaca od strane državnih i lokalnih vlasti, implementacija sustava glasovanja temeljena na tehnologiji lanca blokova ili uvođenje inovativnosti te pokušaj sprečavanja budućih problema te uspostavljanje sigurnog lanca opskrbe hranom ili medicinskim potrepštinama. Vjerojatno će se neki pitati kakve veze i koristi od toga ima država i lokalna samouprava. Možemo se sjetiti početka još aktualne pandemije COVID-19 te poteškoća koja su bila prisutna na lanac opskrbe. Lanac opskrbe se nije još ni oporavio od utjecaja pandemije, a našao se pod pritiskom drugih svjetskih kriza. Vidjelo se da lanac opskrbe ima veliku važnost za svaku državu i države su počele povezivati državne agencije, proizvođače, distributere i prijevoznike. Implementacijom konzorcijskog lanca blokova koji će uključiti sve sudionike, uspostavio bi se pouzdan izvor informacija koji bi povezao poslovnu mrežu i državne agencije. Informacije na toj mreži bi bile uvijek dostupne, istinite, brzo dostupne i postojane. Konzorcijski lanac blokova bi mogao uključivati više agencija, ministarstava pa čak i pojedinca. Ako uzmemo primjer problema s početkom cijepljenja tijekom pandemije COVID-19, distribucija cjepiva i cijepljenje osoba je moglo biti ciljano i kontrolirano (slika 3.1.). U ovom primjeru konzorcijskog lanca blokova potrebna je dozvola za pristup mreži od strane ministarstva zdravstva, zavoda za javno zdravstvo i odabranog liječnika. Konsenzus se postiže verifikacijom određenih sudionika, a dostupnost informacijama je ograničena. Podaci o pacijentu su zaštićeni u lancu blokova, a sudionicima nije u interesu kompromitirati lanac budući da djeluju u najboljoj namjeri.



Slika 3.1. *Uključeni subjekti u lanac opskrbe na primjeru distribucije cjepiva*

Drugi primjer implementacije lanca blokova u sustav e-uprave je estonski primjer e-rezident. Usluga nudi digitalni identitet bilo kome tko želi pokrenuti i voditi posao u Estoniji. E-rezidenti ne stječu automatski pravo na boravak u Estoniji, ali im usluga daje mogućnost da imaju financijski život u toj maloj baltičkoj državi. Estonije je poznata kao država koja je pionir u uvođenju servisa e-uprave koju nudi svojim građanima.

Republika Južna Koreja je putem nacionalnog sustava digitalnog identiteta na mobilnim uređajima, temeljenog na tehnologiji lanca blokova, svojim državljanima omogućila digitalne vozačke dozvole (eng. *mobile driver license*). Svatko tko ima vozačku dozvolu s ugrađenim čipom može kreirati e-vozačku. Kreiranje e-vozačke započinje zahtjevom korisnika nakon čega započinje proces generiranja javnih i privatnih ključevi (slika 3.2.). Korištenjem NFC čitača korisnik verificira svoju vozačku dozvolu unosom 4-znamenkastog koda. Na čipu vozačke dozvole ne nalaze se osobni podaci korisnika već samo ključ, koji se provjerava preko centralnog poslužitelja. Nakon skeniranja lica vozača, predložak lica se uspoređuje s pohranjenim biometrijskim predloškom na centralnom poslužitelju kao i telefonski broj.

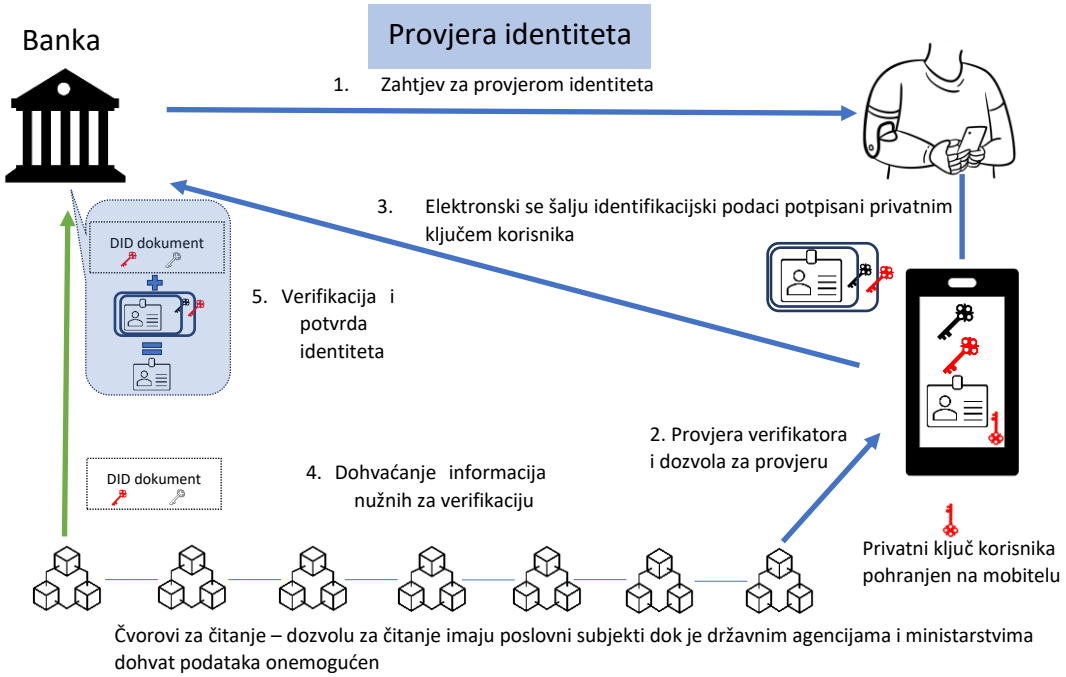


Slika 3.2. *Postupak izdavanja e-vjerodajnice*

Tradicionalna, plastična, vozačka dozvola je i dalje ključna kao jedan od koraka prilikom identifikacije. Budući da su i dalje još važeće vozačke dozvole bez čipa, veliki broj korisnika još nema mogućnost stvaranja digitalne vozačke dozvole. Budući da se na e-vozačkoj dozvoli nalaze svi relevantni podaci o korisniku, korištenje ovog servisa kao zamjena za fizičku vjerodajnicu je našlo svoju širu primjenu. Prilikom korištenja neke od e-usluga državnih službi, u slučaju za potrebom za popunjavanjem elektronskog obrasca, dovoljno je otvoriti aplikaciju digitalne vozačke dozvole i dati privolu za dijeljenjem podataka. Mnoge druge institucije kao što su banke, trgovine, rent-a-car iznajmljivači i sl. spremne su na prihvaćanje digitalne vjerodajnice (slika 3.3.).

Kako bi se osigurali od neovlaštenog pristupa podacima o korisnicima, a radi zaštite privatnosti korisnika, državne službe i agencije imaju također ograničen pristup. Kreiranje digitalnih vjerodajnica, odnosno kreiranje blokova u lancu blokova je trenutno dopušteno samo državnih agencijama (BP čvor), ali pristup čvorovima za čitanje (slika 3.3.) imaju samo poslovni subjekti, dok je državnim agencijama pristup onemogućen. Razlog za takav pristup uveden je kako bi se smirila zabrinutost javnost o nadzoru građana od strane države, te kako bi se onemogućilo državnim agencijama praćenje aktivnosti građanina [15]. Jedan od razloga korištenja tehnologije lanca blokova je kontinuitet pružanja usluge. Decentralizacija usluge je jedan od argumenata korištenja tehnologije lanca blokova budući da su centralizirane usluge

ranjive zbog utjecaja mogućih tehničkih kvarova ili napada na poslužitelj. Razlog zbog kojeg je tradicionalnu plastičnu vozačku dozvolu i dalje nužno posjedovati je mogući gubitak telefona. Naime, u slučaju gubitka mobilnog uređaja na kojem se nalazi digitalna vjerodajnica, moguće je kreirati novu vjerodajnicu na novom uređaju sve dok imamo fizičku vjerodajnicu, u našem slučaju tradicionalnu plastičnu vozačku dozvolu.



Slika 3.3. *Korištenje e-vjerodajnice*

Sustav digitalnog identiteta, bez obzira na kojoj tehnologiji je temeljen, nije sustav bez greške. Više je tu problema koji se pojavljuju, od uključenosti privatnih kompanija u izgradnju ekosustava digitalnog identiteta preko slučajeva u kojima je servis digitalnog identiteta nedostupan pa sve do „tradicionalnih“ nasljeđa sustava pojedinih država i kontrole stanovništva. U primjeru iz Republike Južne Koreje država je sama sebi onemogućila pristup zapisanih informacija o građaninu, dok u primjeru NR Kine imamo slučaj kada država ima tendenciju nadzora građana, a pravo na privatnost se gubi danom rođenja. Sama tehnologija lanca blokova neće zaštiti korisnike od sustava u kojem živi. Također, jedan od nedostataka digitalnog identiteta je nedostupnost servisa u teško dostupnim područjima i među stanovništvom koje nije sklono novim tehnologijama. Izrađeno je nekoliko studija slučaja koje su iznijele zabrinutost za digitalnu isključenost [16]. Zaključak je da, kao u primjeru Južne

Koreje, tradicionalne identifikacijske iskaznice trebaju ostati kako bi se svakom građaninu omogućilo pravo na identitet dok mogućnost digitalnog identiteta treba dati svakom građaninu na izbor.

3.3 Lanac blokova u zdravstvenom sustavu

Učinkovit, ekonomičan i kvalitetan zdravstveni sustava je cilj svake države. Za postići tako nešto potrebno je provesti reforme, a najbezbolnije je krenuti od kvalitetnog upravljanja podacima. Danas je IT tehnologija neizostavni segment svih poslovnih sustava koja, u slučajevima kada je ispravno implementirana i korištena, rezultira velikim uštedama. U svijetu je nekoliko projekata korištenja lanca blokova u zdravstvenom sustavu. Dok su neki u pilot fazi, neki su implementirani, ali svima je zajednička implementacija međuinstitucionalnog elektroničkog zdravstvenog kartona. Pohranjivanje zdravstvenih podataka pacijenta tijekom života pacijenta i dijeljenje podataka je koncept elektroničkog zdravstvenog kartona. Ono radi čega ovaj koncept treba promatrati ozbiljno i na nacionalnoj razini je zaštita privatnosti pacijenata i sloboda izbora. Postavlja se pitanje može li tehnologija lanca blokova olakšati dijeljenje podataka u zdravstvu i u isto vrijeme štititi privatnost pacijenata i omogućiti pacijentu da odlučuje tko će imati pristup kojoj vrsti podataka. Primjer iz Estonije i Južne Koreje nam jasno prikazuje da može. Iz primjera mobilne vozačke dozvole u Južnoj Koreji možemo vidjeti da država sama sebi može zabraniti pristup privatnim podacima. Nemojmo zaboraviti da je ovdje riječ o uređenom i demokratskom društvu.

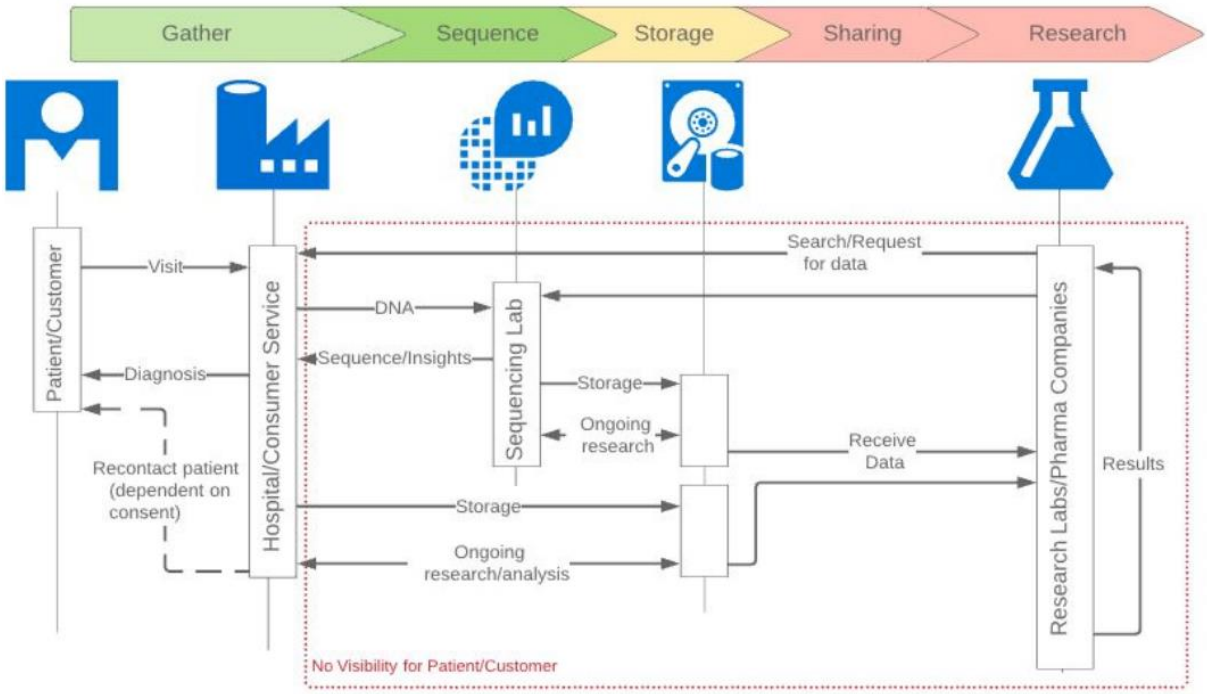
Neki će vjerojatno postaviti pitanje zašto je potrebno uvoditi tehnologiju lanca blokova umjesto relacijskih baza podataka. U Republici Hrvatskoj danas postoji nekoliko digitalnih servisa koji integriraju razne poslovne sustave zdravstvenih institucija u RH međusobno u cilju razmjene podataka. Tako danas imamo e-Zdravstvo, e-Recept, e-Naručivanje, e-ZdravstveniZapis temeljene na relacijskim bazama podataka gdje je matični broj osiguranika identifikacijski atribut na temelju kojeg se radi pretraživanje. Gideona Greenspana iz *MultiChaina* napisao je da „*… ako vaš zahtjev ispunjava današnje relacijske baze podataka, bilo bi ludo koristiti lanac blokova*.“ [17]. Relacijske baze podataka su usavršavane i testirane desetljećima. Međutim, postoje uvjeti kada tradicionalne baze podatak imaju nedostatke. Ti nedostaci su:

- puno subjekata s ovlastima za zapisivanje podataka u bazu,

- puno subjekata s ovlastima za pristup podacima u bazi,
- nepovjerenje među samim subjektima,
- potreba za trećim subjektom radi provjere unesenih podataka.

Svi ovi navedeni nedostaci tradicionalnih baza podataka su argumenti za primjenu lanca blokova. Iako lanac blokova i tradicionalne baze podatak imaju istu namjenu, služe za pohranu podataka, funkcionalno i strukturno se razlikuju jedna od druge. Tradicionalne baze podataka su centralizirane i kontrolirane od strane administratora, dok su lanci blokova decentralizirani i samim time uklanjaju potrebu za administratorom. Time se otklanja mogućnost nepovjerenja među subjektima, a ujedno se decentraliziranjem smanjuju troškovi. Budući da nema centralnog poslužitelja, smanjuje se ranjivost na vanjske prijetnje (zlonamjerni softver, zlonamjerni napadi, prirodne nepogode, tehnički problemi).

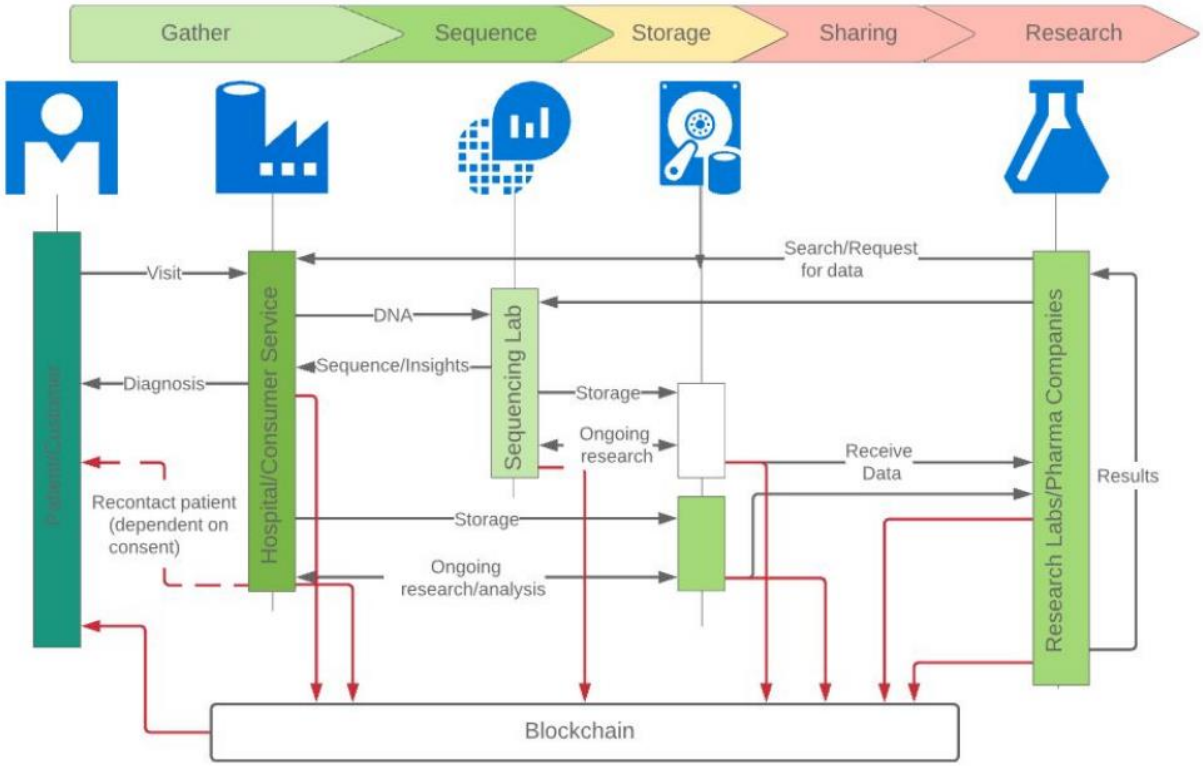
Način na koji danas ekosustav u zdravstvu funkcionira je prikazan na slici 3.4. Vidimo kako se prikupljeni genetski materijal pacijenta šalje na daljnju obradu od strane zdravstvene ustanove ili odabranog liječnika. Pacijent prije toga većinom potpisuje dokumente bez čitanja istih, a koji mogu sadržavati dozvolu za pristup podacima pacijenta od strane trećih lica.



Slika 3.4. *Tradicionalni proces obrade genetskom materijala pacijenta*

Izvor: [18]

Ovdje pacijent ne može upravljati dozvolom pristupa trećim stranama nad rezultatima svojeg genetskog materijala. Primjenom tehnologije lanca blokova, genetski materijal se može „tokenizirati“ i povezati sve entitete u procesu u povratnu petlju, od pacijenta do laboratorija s trećim stranama radi pristupa podacima (slika 3.5.). Pacijent bi putem aplikacije na svojem mobitelu mogao odobravati pristup znanstvenicima, farmaceutskim kompanijama ili drugim klinikama.



Slika 3.5. *Proces obrade genetskog materijala upotrebom tehnologije lanca blokova*

Izvor: [18]

Pacijent bi mogao dobiti dodatne informacije poput, u kojim znanstvenim istraživanjima su njegovi rezultati obrađivani ili povijest svih slučajeva u kojima je bio njegov genetski materijal. Isto tako, pacijent bi sam mogao imati financijsku korist za razliku od tradicionalnog, današnjeg, pristupa kad u najboljem slučaju nema financijski trošak. Također postoji mogućnost da pacijent poveže svoje rezultate s bankom genetskog materijala drugih pacijenta.

Ovako rješavanje problema privatnosti omogućilo bi pacijentima da sami kontroliraju kome će davati podatke, kome će otkriti svoj identitet, a u kojim slučajevima će biti pod pseudonimom.

3.4 Lanac blokova u financijskom sustavu

Mnogo je područja u financijskom sektoru u kojima se tehnologija lanca blokova može primijeniti.

- Tržište kapitala – izdavanje vrijednosnim papirima, trgovanje vrijednosnim papirima,
- Upravljanje imovinom – pokretanje i upravljanje fondovima,
- Bankarstvo – kreditiranja, tuzemne i inozemne transakcije,
- Osiguranje – obrada zahtjeva, isplata, ugovaranje polica.

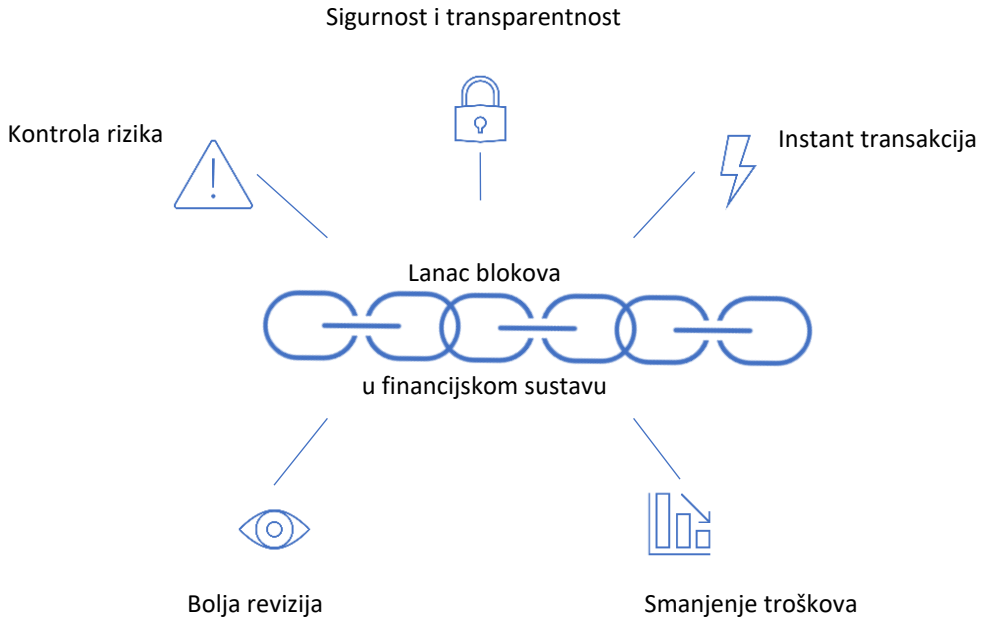
Tradicionalni način obavljanja financijske transakcije zahtjeva potvrdu transakcije treće strane. U većini slučajeva treća strana, posrednik, je financijska institucija koja za navedenu uslugu obračunava i naplaćuje naknadu. Međutim, tehnologija lanca blokova je posrednika učinila nepotrebnim te na taj način prisilila institucije u financijskom sustavu na uvođenje nužnih promjena.

S druge strane globalnim financijskim sustavom dnevno se koriste milijarde korisnika i u njemu se dnevno provedu transakcije u vrijednosti trilijuna eura. To su velike vrijednosti koje ujedno predstavljaju izazov za financijski sustav. Svake godine 45% posrednika iz financijskog sustava (burze, banke ili osiguravajućeg društva) pretrpi ekonomsku štetu uzrokovanu kriminalnom radnjom [19].

Razvoj rješenja na temelju tehnologije lanca blokova za financijski sustav može dovesti do nekoliko koristi. Nabrojat će se samo neke od prednosti:

- decentralizacija financija, DeFi,
- smanjenje troškova i ušteda na vremenu,
- rizik od ljudske pogreške, prijevara i ukupnog rizika je sveden na minimum,
- „tokenizacija“ ili digitalizacija imovine olakšava proces upravljanja i trgovanja, pristup tržištima i dodatnu likvidnost,
- privatnost je jedna od prednosti lanca blokova,
- izvođenje transakcija u stvarnom vremenu, brzo i sigurno,
- brža procjena kreditnog rizika,
- automatizirana obrada zahtjeva pomoću pametnih ugovora,
- automatizirana isplata kreditnih zahtjeva, police osiguranja ili isplata dobiti.

Financijski sustav je godinama suočen s mnogim izazovima. Nove tehnologije rješavaju probleme, ali u isto vrijeme stvaraju nove probleme u procesu. Zbog toga tehnologija lanca blokova može pomoći u rješavanju glavnih izazova s kojima se financijski sustav suočava (slika 3.6.).



Slika 3.6. *Izazovi s kojima se financijski sustav suočava*

3.4.1 Sigurnost i transparentnost

Financijski podaci tijekom procesa obrade prolaze kroz nekoliko točaka obrade od strane posrednika prije nego se spreme u centraliziranim bazama podataka. Takav sustav je netransparentan, a sigurnost podataka isključivo ovisi o posrednicima i sigurnosti baze podataka. Čak i ako je baza podataka maksimalno zaštićena, ipak ovisi o čovjeku, što se do danas pokazalo kao najslabija točka svakog sustava. Nedostatak transparentnosti sustava je ujedno sigurnosna prijetnja budući da se za propust sazna kad se prijetnja dogodi. Uvođenjem tehnologije lanca blokova u financijski sustav rješava se problem transparentnosti i sigurnosti:

- Nepromjenjivost – podaci se ne mogu mijenjati.
- Privatnost – korištenje sigurnosnih ključeva – javni i privatni ključ. Javni ključ je dostupan svih korisnicima. Pomoću javnog ključa transakcija će biti vidljiva svim

sudionicima u mreži dok će detalji o transakciji biti vidljivi samo onima s privatnim ključem. Ovime je sustav transparentan dok istovremeno štiti povjerljive podatke sudionika transakcije.

- Tehnologija dokaz znanja bez znanja (eng. *zero-knowledge proof*) – omogućava provjeru financijskih podataka bez otkrivanja dodatnih informacija. To je metoda kojom jedna strana može dokazati drugoj strani da je određena izjava istinita bez otkrivanja dodatnih informacija osim činjenice da je izjava doista istinita [20].

3.4.2 Smanjenje troškova

Budući da je financijski sustav centraliziran, mnogo se ulaže u održavanje i sigurnost baze podatka. Ti troškovi su obično ponavljajući troškovi što sustav čini skupljim, a opet ne postoji jamstvo da do pada sustava ili povrede podataka neće doći. Prema nekim istraživanjima, tehnologija lanca blokova može smanjiti troškove u financijskom sustavu do 20 milijardni dolara godišnje [21]. Ujedno bi implementacija pametnih ugovora u njihove sustave dodatno smanjila posredničke i knjigovodstvene troškove.

3.4.3 Učinkovita kontrola rizika

Kreditiranje je jedna od primarnih usluga financijskih ustanova, a nenamjenski krediti su krediti s vrlo visokim rizikom budući da se ne ugovaraju sredstva osiguranja. Zbog toga postoji visok rizik od neispunjavanja ugovornih obveza strane koja koristi kreditna sredstva. Kod namjenskih kredita postoji rizik od nekorištenja kredita u namjenske svrhe budući da nadzor i praćenje korištenja kredita obavljaju posrednici, a ne poslovne banke koje su isplatile sredstva. Tehnologija lanca blokova bi, definiranjem svakog sudionika u kreditu kao čvora, eliminirala potrebu za posrednikom. Bilježenjem svake transakcije na mreži smanjili bi se kreditni rizici, a uvođenjem pametnih ugovora ubrzao bi se proces obavljanja transakcija. Također zbog nemogućnosti mijenjanja podataka, sustav je pouzdaniji u odnosu na tradicionalni financijski sustav.

3.4.4 Instant transakcija

U današnje vrijeme za obavljanje međunarodne transakcije potrebno je nekoliko dana dok sredstva ne budu vidljiva na računu. Razlog zbog čega se to događa je što u procesu izvršavanja transakcije postoji nekoliko posrednika čije sudjelovanje doprinosi sigurnosti centraliziranog sustava dok na drugu stranu usporava proces i povećava troškove. Lanac blokova je točka prema točki mreža, gdje je sudjelovanje posrednika nepotrebno, a umjesto njih će pametni ugovori upravljati transakcijama. Na ovaj bi se način izvršenje transakcije u međunarodnom prometu moglo realizirati u realnom vremenu.

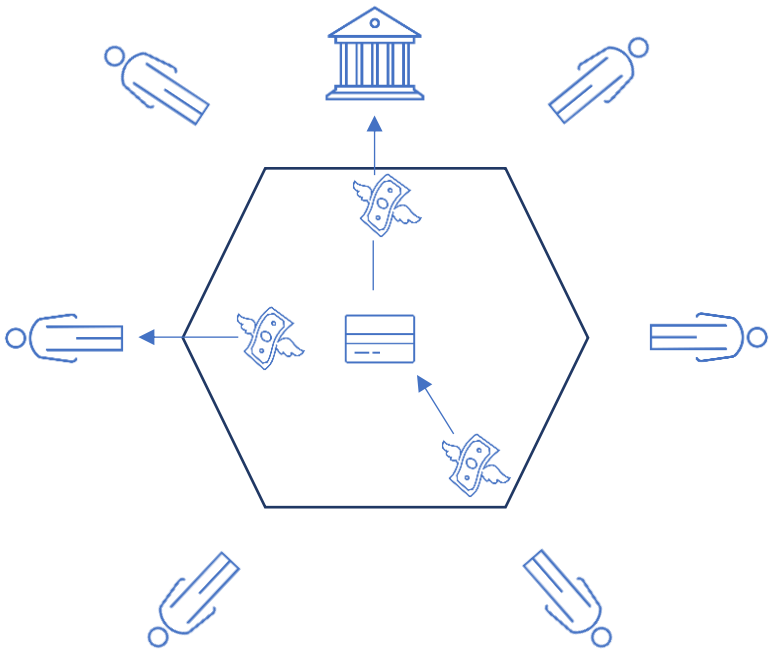
3.4.5 Kvalitetnija financijska revizija

Revizija je proces koji je dug i skup. Prilikom pripreme revizije prikupljeni podaci mogu biti slučajno ili namjerno izmijenjeni zbog čega može doći do financijskih gubitaka. Budući da su podaci u lancu blokova nepromjenjivi, revizori bi mogli na jednostavan način provjeriti ispravnost podataka što bi pojednostavilo postupak revizije, a sam postupak revizije bi se smanjio. Lanac blokova nam donosi transparentnost što revizoru daje mogućnost praćenja svake sumnjive transakcije.

3.5 Lanac blokova u sektoru prodaje

Sektor prodaje je jedan od najdinamičnijih sustava u kojem su se, tehnološkim napretkom u zadnjim desetljećima, pojavile nove metode prodaje. Napretkom u logistici i transportu, sektor prodaje je uvelike doprinio rastu svjetske trgovine zajedno s globalizacijom. Tijekom pandemije COVID-19 najznačajniji kanal prodaje činila je prodaja putem interneta. Tehnologija lanca blokova može doprinijeti u rješavanju problema koje prodaja putem interneta čine ranjivima. Prvenstveno se misli na sigurnosni aspekt prilikom plaćanja putem interneta, koji je jedan od neizostavnih koraka kod korištenja ovog vida kanala kupnje, i zaštita privatnosti kupaca kod personaliziranih ponuda. Dok tradicionalni sustav plaćanja zahtijeva prisustvo treće strane kao posrednika, kod internet trgovine posrednik je banka (slika 3.7.), tehnologija lanca

blokova izbacuje posrednika iz sustava plaćanja. To rezultira sigurnijom kupnjom i smanjuje troškove budući da se posredničke usluge ne naplaćuju.



Slika 3.7. *Tradicionalni sustav plaćanja uključuje treću stranu*

Sigurnost podataka i provjera identiteta kupca jedan su od najvećih izazova internet trgovine. Sustav plaćanja točka prema točki je rješenje koje sa sobom donosi tehnologija lanca blokova. Decentralizacija, sigurnost identiteta i brzina izvršenja transakcije su rezultati uvođenja tehnologije lanca blokova u sustav plaćanja putem interneta:

- Decentralizacija – decentralizirani podaci nisu u vlasništvu treće strane. Trgovci i kupci su strane u sustavu plaćanja koje su izravno uključene i koje same mogu kontrolirati transakciju.
- Sigurnost identiteta – korištenjem lanca blokova sva plaćanja, povijest kupovine i osobni podaci su transparentni u sustavu.
- Brzina izvršenja transakcije – za izvršiti transakciju korištenjem tehnologije lanca blokova potrebno je svega nekoliko minuta, dok se prilikom tradicionalnog plaćanja putem interneta transakcija najprije mora autorizirati, a zatim potvrditi. To može potrajati nekoliko dana, pogotovo ako se kupuje u vrijeme vikenda i praznika.

Drugi problem s kojim se internet trgovine suočavaju je problem u opskrbnom lancu i upravljanjem zalihama. Uvođenjem tehnologije lanca blokova u opskrbnom lancu, trgovci mogu smanjiti troškove, osigurati privatnosti i povećati sigurnost informacija u poslovnom procesu. Manji troškovi se tehnologijom lanca blokova ostvaruju izbjegavanjem posrednika u lancu što ujedno smanjuje rizike od gubitka informacija. Pohranjivanjem podataka o proizvodima u lancu blokova, informacija o proizvodima, praćenja proizvoda i narudžbi, onemogućeno je mijenjanje podataka. Također pomoću tehnologije lanca blokova je pojednostavljen proces praćenja podrijetla proizvoda.

Do sada smo promatrali kako tehnologija lanca blokova utječe na sigurnost i privatnost podatka kod trgovca. Kakve koristi od uvođenja lanca blokova ima kupac? Osim sigurnije kupnje koju lanac blokova omogućava decentralizacijom i pristupom točka prema točki u kojoj nema više posrednika, tehnologija lanca blokova daje mogućnost kupcu da sam odlučuje tko može vidjeti povijest kupovine i odrediti trgovce kojima se dopušta slanje promotivnih materijala na njihovu elektroničku poštu. Do sada je kupac često bio suočen s velikim brojem neželjenih poruka, tzv. *spam* poruka, i reklamnim materijalima na svojoj elektroničkoj pošti. Kupcima je navedeno iskustvo često neugodno s čime gube povjerenje u trgovca, a velika količina neželjenih poruka povećava sigurnosni rizik kod kupca od zlonamjernog napada. Ovo je rezultat tradicionalne internet trgovine i curenja osobnih podataka. Pružiti mogućnost kupcu da odlučuje o tome tko može imati pristup njegovim aktivnostima u konačnici će rezultirati zadovoljnijim kupcem i boljoj ocjeni prilikom recenzije trgovca ili proizvoda i privlačenju novih kupaca. Tehnologija lanca blokova također onemogućava davanje recenzija od nepostojećih kupaca budući da svaki kupac ima svoj ID, a provjera podataka se obavlja prilikom registracije. Nakon provjere, kreira se blok koji se dodaje u lanac nakon što je verificiran od strane čvorova u mreži. Zbog takvog pristupa, informacije u lancu blokova se ne mogu mijenjati niti brisati.

Uvođenje tehnologije lanca blokova u proces prodaje putem interneta dodatno će smanjiti mogućnosti prijevara. Osim trgovaca kupci također imaju koristi od internet trgovine temeljene na lancu blokova u vidu bolje kontrole privatnih informacija, izbjegavanje neželjenih poruka i kvalitetnije povratne informacije.

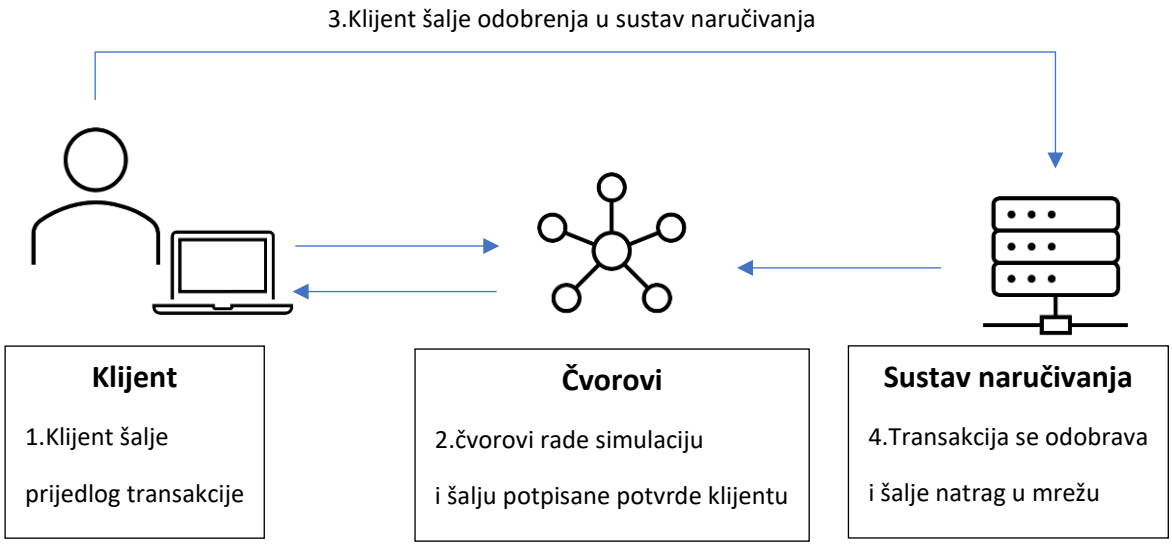
3.6 Lanac blokova u B2B poslovnom sustavu

Svaki B2B model izgrađen je na vezi između dva ili više poslovnih subjekata, naprimjer poslovni odnos između proizvođača i distributera ili distributera i trgovca. Njihova veza je međusobno ovisna i u tom lancu bitna je dobra organizacija kako bi svi učinkovitije poslovali. B2B aktivnosti se obično odvijaju mrežno i karakteristika njihovih transakcija su velike količine naručene robe i dugoročni ugovori koji su rezultat složenih pregovora. Cilj B2B modela je zadovoljiti sve međusobno povezane strane pa stoga učinkovitije poslovanje u B2B modelu doprinosi financijskoj uštedi, smanjuje vrijeme zastoja i optimizira rad.

Na tržištu danas postoje programska rješenja temeljena na tehnologiji lanca blokova, a čija upotreba ima povoljne učinke na poslovni proces unutar poslovne mreže. *TrendeLens* je logistički sustav, razvijen na Hyperledger Fabric platformi i služi za automatizaciju lanca opskrbe i pojednostavljuje isporuku. Hyperledger Fabric platforma je okvir lanca blokova otvorenog koda i sastoji se od članova koji međusobno komuniciraju na mreži. Sudionici jednog poslovnog procesa čine ekosustav s kontroliranim pristupom, pristupaju putem pozivnice i unaprijed definiranim ovlastima. Naprimjer, organizacija može biti proizvođač u mreži koja se sastoji od poslovnih partnera u lancu opskrbe. Svaka organizacija u mreži je definirana korijenskim certifikatom specifičnim za tu organizaciju. Korisnici i drugi sudionici, naprimjer ravnopravni čvorovi, u toj organizaciji posjeduju certifikate koji su izvedeni iz korijenskog certifikata. Svaki certifikat u mreži definira ovlasti za svaki entitet, od pristupa samo čitanju do potpunog pristupa. Korijenski certifikat je pohranjen u tijelu za izdavanje Fabric certifikata (CA). Tijek narudžbe u sustavu temeljenom na Hyperledger Fabric platformi je sljedeći (slika 3.8.):

1. Klijentska aplikacija šalje prijedlog narudžbe, transakciju, čvorovima unutar organizacije na odobrenje.
2. Čvorovi provjeravaju identitet klijenta koji je poslao transakciju i njegove ovlasti. Zatim se radi simulacija na temelju poslane transakcije i ako je rezultat simulacije u skladu s očekivanim rezultatom, klijentu se šalje potpisana potvrda transakcije.
3. Klijent prikuplja potpisane potvrde od čvorova te nakon što prikupi definirani broj potpisanih potvrda, transakciju šalje u proces narudžbe.
4. Prilikom narudžbe sustav provjerava ima li transakcija odgovarajući broj potpisanih potvrda u skladu s politikom potvrda. Odobrene se transakcije kronološki poredaju u

blokove i šalju se čvorovima u mreži na konačnu provjeru nakon čega se dodaju u knjigu.



Slika 3.8. *Proces naručivanja u sustavu temeljenom na Hyperledger Fabric platformi*

Danas su poslovni subjekti još skeptični kada je riječ o digitalizaciji. Mnogi još smatraju da je digitalizacija korištenje elektroničke pošte ili internet bankarstva, ali potpuna digitalizacija podrazumijeva spremanje dokumenata na digitalne platforme. Zabrinutost poslovnih subjekata zbog potencijalnog izlaganja sigurnosnim rizicima je opravdana, ali oklijevanje i zanemarivanje nadogradnje sustava novijim tehnološkim dostignućima znači nastavak dosadašnje prakse koja je jednako, ako ne i više, rizična. U primjeru procesa naručivanja, opisanog na prethodnoj slici te temeljenog na još aktualnoj praksi naručivanja putem elektroničke pošte možemo vidjeti:

1. Klijent šalje dokument osobi zaduženoj za naručivanje putem elektroničke pošte.
   Prijetnja 1: Klijentsko računalo je zaraženo zlonamjernom aplikacijom i dokument je lažan ili izmijenjen.
2. Osoba zadužena za narudžbu je dobila dokument od klijenta
   Prijetnja 1: Narudžba je stigla sa zaraženog računala kao rezultat napada.
   Prijetnja 2: Podaci u narudžbi su izmijenjeni kao rezultat zlonamjerne aplikacije na računalu.

Prijetnja 3: Računalo osobe zadužene za narudžbu je zaraženo i narudžba je izmijenjena prilikom primitka.

3. Osobe nemaju običaj provjeravati stvarni identitet u poslovnom lancu što je samo po sebi prijetnja. Nerijetko se događa da poslovni subjekti dobiju legitimnu fakturu s izmijenjenim bankovnim podacima nakon čega izvrše plaćanje legitimne fakture na bankovni računa zlonamjernog napadača.
4. U prethodnim koracima su izvršene prijetnje korištenjem metoda presretanja, lažiranja ili instalacijom zlonamjernog softvera. Najčešće zbog ljudske nepažnje sve ove metode su se mogle izvršiti u bilo kojem koraku. Čak i kad je proces naručivanja završen, slanjem elektroničke pošte na adresu osobe zadužene za plaćanje, moguće je usmjeriti plaćanje na krivi račun. A sve zbog nepostojanja prakse provjere identiteta i istinitosti podataka.

Tehnologija lanca blokova osigurava nepromjenjivost i sljedivost šifriranih zapisa. Sustavi izgrađeni na Hyperledger Fabric platformi koriste tzv. dozvoljeni lanac blokova koji daje mogućnost odabira članova, razinu pristupa i razinu kontrole. Takvi sustavi čine poseban ekosustav, mrežu s pozivnicom. Korisnici pristupaju ekosustavu nakon temeljitih provjera i s definiranom politikom pristupa čime se onemogućuje pristup zlonamjernim korisnicima takvim ekosustavima.

Treba također voditi računa da je lanac blokova samo jedan dio sigurnosnih rješenja. Ekosustavi, unatoč korištenju tehnologije lanca blokova, moraju koristiti najnaprednije metode autentifikacije, komunikacija se mora odvijati korištenjem minimalno TLSv1.2 protokola, a sama mreža u kojem se nalaze sustavi moraju biti zaštićeni vatrozidom.

Budući da takovi ekosustavi sadrže osobne podatke, zadovoljavanje GDPR standarda je nužnost. Ali za sada ovdje nailazimo na problem brisanja osobnih podataka prema uputama GDPR standarda. Također, jedan od argumenata za pouzdanost ovakvih ekosustava, je tendencija proizvođača da kontinuiranim unapređenjem sigurnosnih mehanizama, uvođenjem sigurnosnih kontrola i kontinuiranim provjerama provode sigurnosne provjere i procjenu rizika nad sustavom. Usklađenost s međunarodnim sigurnosnim standardima dodatno jamči sigurnost ovakvih ekosustava.

Trenutni sustav upravljanja opskrbnim lancem ima nekoliko problema koji se pokušavaju riješiti korištenjem tehnologije lanca blokova. Cilj svih projekata je izgraditi transparentan

lanac opskrbe pomoću kojeg će kupci imati uvid u tijek narudžbe, a čime će se povećati povjerenje kupaca.

4. Slabosti, ranjivosti i napadi na lanac blokova

Prije nego krenemo u iznošenje slabosti, ranjivosti i napada na lanac blokova, napravit će se usporedbu lanca blokova s bazom podataka. Na početku je spomenuto da je lanac blokova vrsta baze podataka, ali ovdje se želi naglasiti da imaju istu primjenu. I lanac blokova i baza podataka pohranjuju imovinu, informaciju, koja ima određenu vrijednost i koju pokušavamo zaštiti, a kojoj zlonamjerni korisnik pokušava pristupiti.

Lanac blokova je decentralizirana baza podataka koja u primjeru privatnog lanca blokova može biti centralizirana dok je baza podataka centralizirana i kontrolirana od strane administratora. Lanac blokova koristiti arhitekturu mreže distribuirane knjige i podržava samo operacije pisanja i čitanja podatka dok baza podataka koristi klijent-server arhitekturu i podržava CRUD (kreiranje, čitanje, izmjena i brisanje). Implementacija lanca blokova u odnosu na baze podataka skuplja je s daleko višim troškovima održavanja, a administratorske ovlasti u lancu blokova su nezamislive. Zbog nepostojanja administratorskih ovlasti nad lancem blokova te nemogućnosti izmjene i brisanja podataka, integritet podataka je zajamčen dok su podaci u bazi podataka ranjivi na zlonamjerne namjere. Baze podataka nisu transparentne i osoba s administratorskim ovlastima može odlučiti tko i kojim podacima se može pristupiti dok u isto vrijeme jedna od prednosti lanca blokova je upravo transparentnost. Prednost baze podataka u odnosu na lanac blokova je brzina i skalabilnost. Zapisivanje i pristup podacima u lancu blokova su usporeni zbog potrebe za verifikacijom i korištenja konsenzusa.

Ako netko napadne i kompromitira bazu podatka, te podatke će probati prodati na crnom tržištu. Ali ako netko izvrši napad na kriptonovčanik, to doslovno znači da je novac u novčaniku napadača.

4.1 Slabosti lanca blokova

Postoje brojni projekti koji pokušavaju obuhvatiti sve slabosti lanca blokova. Najviše na tom području radi i čini Ministarstvo domovinske sigurnosti SAD-a koji ujedno i sponzoriraju takve napore, *Common Weakness Enumeration* bazu (https://cwe.mitre.org/) i *SWC* registar (https://swcregistry.io/). Trenutno *Cloud Security Alliance* (https://docs.google.com/spreadsheets/d/1HIM3BH8Cgth27ED4ruy9fXOpbOUAPAGY7merl

ZiE6_U/edit#gid=1028635246) nastoji objediniti i dokumentirati sve slabosti lanca blokova i pametnih ugovora na jednom mjestu, čime bi se omogućilo razvojnim programerima, sigurnosnim inženjerima i revizorima razumijevanje ranjivosti i ispravljanje slabosti prije nego ih zlonamjerni korisnik pronađe.

Tehnologija lanca blokova je sama po sebi sigurna i sustavi koji u svom radu koriste tehnologiju lanca blokova su sigurniji, ali ne bez slabosti. Ovo su neke od slabosti lanca blokova:

- mogućnost kreiranja lažnih mrežnih čvorova,
- mogućnost kreiranja zlonamjernih čvorova,
- krajnje točke i sigurnost krajnjih točaka,
- mogućnost preuzimanje kontrole nad natpolovičnom većinom čvorova na mreži,
- *phishing* napad nad korisnikom,
- slabi privatni ključevi i njihova neadekvatna pohrana.

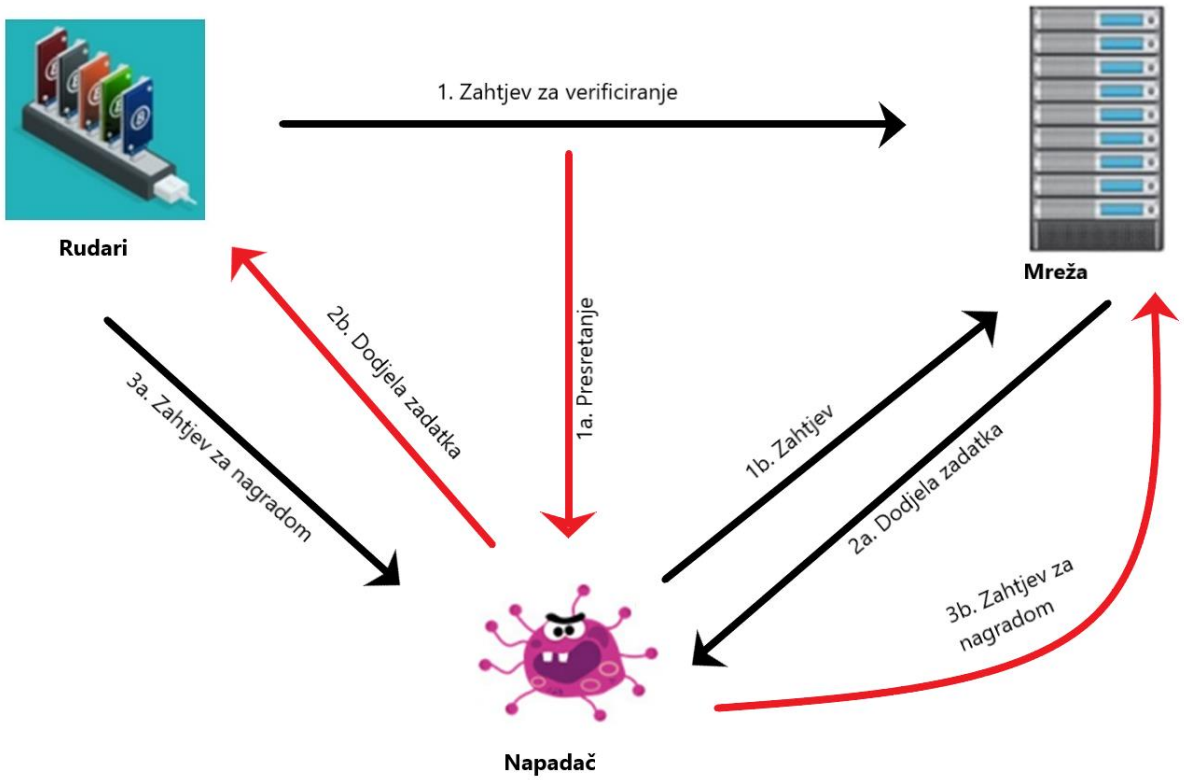
Nabrojane slabosti su rezultat nenadziranog pristupa mreži lanca blokova što dovodi do zaključka da, u slučaju mogućnosti provjere identiteta sudionika, implementaciji kontrole pristupa i uspostavljanjem višerazinske razine ovlasti pristupa, slabosti se znatno umanjuju. Sve navedene kontrole nam omogućava privatna mreža lanca blokova, u odnosu na javnu mrežu lanca blokova, pa stoga možemo zaključiti da privatni lanci blokova sadrže manje slabosti u odnosu na javne lance blokova unatoč tome što obje koriste istu tehnologiju lanca blokova. Pristupanjem mreži s pozivnicom, provjera identiteta prije pristupanja i višerazinske ovlasti su kontrole čijim uvođenjem bi se otklonile ili smanjile slabosti ekosustava. Ključni faktor u svim ovim slabostima je čovjek i nedavni napadi na lanac blokova nisu bili toliko usmjereni na tehnologiju, već na osnovne ljudske ranjivosti. *Phishing* napadi, ranjivosti krajnjih točaka ili krađa privatnih ključeva su sve prijetnje usmjerene na iskorištavanje ranjivosti čovjeka te možemo zaključiti da najveća slabost tehnologije lanca blokova sam čovjek.

Ako promatramo samu tehnologiju lanca blokova, sva istraživanja predstavljaju prednosti tehnologije i njezinu sigurnost. Slabosti se neće iznositi, ne zato što ih nema, već zato što nisu pronađene. Stoga ta mladost tehnologije lanca blokova je njezina najveća slabost. Razvojem novih sustava korištenjem tehnologije lanca blokova i stvaranjem novih ekosustava doprinijet će se sazrijevanju tehnologije i uklanjanju slabosti.

4.2 Ranjivosti lanca blokova

Ranjivosti lanca blokova se razlikuju s obzirom na to radi li se o javnom ili privatnom lancu blokova. Još ćemo jednom spomenuti da je javni lanac blokova mreža otvorenog tipa i daje mogućnost svakom korisniku da se pridruži kao anonimni članovi. Javni lanac blokova koriste računala, povezano na internet, radi provjere valjanosti transakcija uz postizanje konsenzusa. S druge strane, privatni lanac blokova je mreža kojoj pristupaju članovi nakon provjere identiteta i uz kontrolirani pristup. Primjer, tvrtka za investicijsko bankarstvo, *JP Morgan*, koristi privatnu mrežu lanca blokova za pojednostavljenje, racionalizaciju i provjeru transakcija i ugovora [22]. Nekoliko čimbenika doprinosi ranjivosti unutar sustava lanca blokova. Najkritičnija komponenta sigurne i decentralizirane knjige lanca blokova je čvor, odnosno računala koja sudjeluju u mreži. Ako jedan od čvorova ne koristi odgovarajuće sigurnosne protokole ili jednostavno koristi zlonamjerni korisnik, podaci koji prolaze kroz lanac blokova podložni su napadu. Ovime je predodžba o inherentnoj sigurnosti lanca blokova narušena kao i sigurnost informacija unutar blokova. Također nedosljednost sigurnosnih protokola između čvorova mreže lanca blokova predstavlja sigurnosnu prijetnju za svaki čvor u mreži.

Danas postoje nekoliko različitih protokola koji šifriraju informacije prilikom razmjene paketa putem interneta. Taško je vjerovati da bi nova tehnologija koristila neki drugi vid komunikacije između sudionika nego protokol koji osigurava privatnost poruke i njezinu autentičnost. Sigurnost lanca blokova ovisi o protokolu koji koristi mehanizam konsenzusa. Za komunikaciju između sudionika unutar mreže, koja koristi konsenzusni algoritam dokaza o radu (PoW), koristi se Stratum protokol. Stratum protokol dopušta sudioniku mreže da kreira „poslove“ za svakog sudionika rudarenja. Problem Stratum protokola je što nije šifriran. Svi poslovi dodijeljeni rudarima, svi rezultati završenih poslova rudara, pa čak i inicijalna autentifikacija, prenose se u čistom tekstu. Dizajneri Stratum protokola, prilikom kreiranja protokola su donijeli ovakvu odluku u dizajnu protokola isključivo radi uštede resursa rudara, budući da bi korištenje SSL ili TLS trošilo hardverski resurs rudara. Navedeno rješenje je omogućilo ranjivost u lancu blokova budući da se promet može prisluškivati, čime se narušava privatnost sudionika ili se MiTM napadom (eng. *Man-in-the-middle* – čovjek u sredini) može manipulirati porukama te omogućiti napadaču da „ukrade“ nagradu (slika 4.1.).



Slika 4.1. *MiTM napad na Stratum protokol*

Prisluškivanjem komunikacije između rudara i mreže, napadač preotima ostvarenu TCP vezu. Kada napadač detektira poruku o dodjeli posla iz mreže, presretne poruku i izmijenjenu proslijedi legitimnom rudaru. Žrtva rudar primljenu poruku o dodjeli posla smatra legitimnom te kreće s rudarenjem. Nakon obavljenog posla, žrtva rudar kreira novu poruku koja sadrži izračunatu naknadu za obavljeni posao i šalje je u mrežu. Napadač presreće poruku i modificira na način da korisničko ime žrtve rudara zamijeni svojim korisničkim imenom i takvu pošalje u mrežu. Također prosljeđuje oštećenu kopiju originalne poruke u mrežu kako bi se osiguralo njezino odbijanje [23]. Ova ranjivost je poznata godinama, a jedno od rješenja je dodavanje autentifikacije u protokol. Problem je što ni jedan od prijedloga za sigurnije rješenje nije globalno usvojeno.

Sljedeća ranjivost s kojem je globalna zajednica upoznata i koja je stvarna prijetnja je ranjivost PoW konsenzusnog algoritma na 51% napad. Ako jedan entitet kontrolira više od 51% resursa mreže, tada taj entitet može modificirati lanac blokova na nedopušten način. Promjena topologije mreže lanca blokova kojom zlonamjerni napadač stječe kontrolu nad mrežom može se izvršiti i na druge vrste lanca blokova koje ne koriste PoW konsenzusni algoritam na način

da se dodaju zlonamjerni čvorovi. Danas kada je podizanje virtualne instance u oblaku svakome dostupno i jeftino, kreiranje i dodavanje novih čvorova koje kontrolira jedna osoba predstavlja stvarnu prijetnju. Za ovakve napade trenutačno ne postoji poznato rješenje bez da se centralizira mreže.

Prema istraživanju iz 2017. godine, 60% cijelog bitcoin prometa se odvija preko samo tri ISP pružatelja usluge [24]. U srpnju 2021. pola od svih bitcoin javnih čvorova imalo je IP adrese iz Njemačke, Francuske i SAD-a, od čega su na prve četiri pozicije podatkovni centri (*Hetzner*, *OVH*, *Digital Ocean* i *Amazon AWS*). Država u kojoj se nalazi najviše čvorova su SAD, otprilike jedna trećina, zatim Njemačka (25%), Francuska (10%), Nizozemska (5%) i Kina (3%). Također, u isto vrijeme, otprilike polovica cjelokupnog bitcoin prometa je preusmjerena na Tor mrežu [25]. Ovi podaci predstavljaju potencijalnu ranjivost budući da se ISP telekomi i podatkovni centri mogu bilo kojem čvoru uskratiti uslugu. Iz ovoga možemo zaključiti da je mrežna infrastruktura jako bitna kod tehnologije lanca blokova. Sigurnost zapisa u bloku je neupitna, budući da su šifrirani i potpisani, međutim promet između čvorova, i u prethodno spomenutom slučaju bitcoin mreže, nije šifriran. Takav se može promatrati od strane telekom operatera ili samih vlada i upravljati s njime.

Korištenje starijih verzija softvera, njihovo neažuriranje, također utječe na ranjivost mreže lanca blokova. Radi smanjenja ranjivosti bitno je da svi čvorovi mreže koriste iste i ažurirane verzije softvera, inače se mogu pojaviti greške u konsenzusu što može dovesti do račvanja lanca blokova.

4.3 Vrste napada i studije slučajeva

4.3.1 Exchange napad

U trenutku pisanja ovog specijalističkog rada, na dan 22. siječnja 2023., dnevna trgovina u mjenjačnicama kriptovaluta ima vrijednost od preko 55 milijardi dolara [14]. Tako veliki promet mjenjačnica kriptovaluta je veliki motiv napadačima. Procjena je da su mjenjačnice u razdoblju od 2011. do 2020. pretrpjele štetu u iznosu od preko 41 milijardu dolara.

Od 2012. godine najmanje 47 mjenjačnica kriptovaluta je pretrpjelo velike kibernetičke napade, a prvi veliki organizirani napad na mjenjačnicu kriptovaluta je izveden 2014. godine.

Mjenjačnica *Mt. Gox* je bila prva centralizirana bitcoin mjenjačnica koja je pretrpjela štetu u višemilijunskom iznosu, izgubila je 850 000 bitcoina u vrijednosti od 460 milijuna američkih dolara. Ukupna vrijednost ukradenih kriptovaluta iz kriptomjenjačnica od 2012. iznosi gotovo 2,72 milijarde [26]. Budući da mjenjačnice kontinuirano ulažu u sigurnosnu politiku svojih ekosustava, ciljevi napadača su postali korisnici mjenjačnica kao najslabija točke svakog sustava koristeći tehnike napada društvenim inženjeringom i shemom povjerenja.

Napad na mjenjačnicu *Mt. Gox* je registriran u veljači 2014. godine i otkriveno je da mjenjačnica bila kompromitirana još od 2011. godine. Napadači su još 2011. godine kompromitirali račun koji je pripadao Jed McCalebu, bivšem vlasniku koji je imao administrativni pristup sustavima mjenjačnice. Tijekom napada napadači su stvorili veliki broj lažnih bitcoinova, a zatim su mjenjačnicu preplavili umjetnom ponudom. Kao rezultat toga, cijena bitcoina u mjenjačnici je pala s 17,50 $ na 1 cent što je omogućilo napadačima kupnju i povlačenje najmanje 2000 pravih bitcoinova prije nego što je mjenjačnica obustavila trgovanje. Tek u veljači 2014. je otkriveno da je mjenjačnica bila ugrožena od 2011. i da su napadači ukrali stotine tisuća bitcoinova u razdoblju od tri godine.

Kronologija događaja u veljači 2014. [27]:

- 7. veljače 2014. - Mjenjačnica *Mt. Gox* obustavlja sva povlačenja bitcoina sa sljedećim priopćenjem: „Greška u softveru daje mogućnost korisniku da koristi bitcoin mrežu za promjenu detalja transakcije kako bi izgledalo da se slanje bitcoina iz novčanika nije dogodilo, a zapravo se dogodilo.“
- 17. veljače 2014. - povlačenja bitcoin sredstava su još uvijek obustavljena dok je mjenjačnica poduzimala koraka u rješavanju sigurnosnih problema.
- 23. veljače 2014. – Mark Kerpeles podnosi ostavku na mjestu glavnog izvršnog ravnatelja bitcoin mjenjačnice *Mt. Gox*.
- 24. veljače 2014. – trgovanje mjenjačnice je obustavljeno, a web stranica mjenjačnice je nedostupna. Iz internog dokumenta koji je procurio van, tvrtka je bila nesolventna nakon što je izgubila 744 408 bitcoina (tablica 4.1.) [28].

Tablica 4.1. *Financijska imovina i obveze Mt. Gox nakon napada*

<table>
<tr><th></th><th>Assets</th><th>Liabilities</th></tr>
<tr><td>Bitcoins</td><td>2,000 BTC in the Hot Wallet</td><td>624,408 BTC (Customers)
+120 000 (MtGox)
-80 208 BTC
From banned or suspicious accounts</td></tr>
<tr><td rowspan="3">Fiat</td><td>22,430,000 USD
In the bank account
(averaged across currencies)</td><td rowspan="3">55,000,000 USD (but still unclear at this point)</td></tr>
<tr><td>5,000,000 USD
held by CoinLab</td></tr>
<tr><td>5,000,000 USD
held by DHS</td></tr>
<tr><td>Total</td><td>32,430,000 USD + 2,000 BTC
(MtGox av price 160 USD = 320,000 USD)</td><td>55,000,000 USD + 744,408 BTC
(MtGox av price 160 USD = 119,105,280 USD)</td></tr>
</table>

Izvor: [29]

- 25. veljače 2014. – *Mt. Gox* mjenjačnica objavljuje odluku na svojim internet stranicama da se obustavljaju sve transakcije kao posljedica nedavnih događaja.
- 28. veljače 2014. – mjenjačnica *Mt. Gox* podnosi zahtjev za zaštitu od bankrota u Tokiju, a 9. ožujka podnosi isti zahtjev u SAD-u.

U to vrijeme putem *Mt. Gox* mjenjačnice obavljalo se 70% svih bitcoin transakcija. Ovaj napad je do dana današnjeg najveća pljačka bitcoina u povijesti. Ukupno je Mt. Gox izgubio oko 750 000 korisničkih bitcoina i 100 000 vlastitih bitcoina, što je u to vrijeme činilo gotovo 7% svih bitcoin kovanica koje su tada bile u opticaju. Važno je spomenuti da korisnički gubici nisu kompenzirani iako je 20. ožujka 2014. prema objavi *Mt. Goxa* pronađen novčanik s približno 200 000 bitcoina [30].

Iz prvog zabilježenog napada na mjenjačnicu kriptovalute može se primijetiti, da pored loše sigurnosne politike koju je mjenjačnica provodila, drugi problem koji je proizašao taj da, u

odnosu na klasično bankarstvo, sredstva klijenata nisu zaštićena. U klasičnom financijskom poslovanju depozita klijenata u uređenom financijskom sustavu postoje regulatorna tijela i agencije koje do određenog iznosa nadoknađuju gubitak klijenta u slučaju bankrota banke. Budući da kriptovalute nisu pod nadzorom ni jedne državne agencije i regulatornog tijela, sav rizik gubitka se prebacio na same klijente. Napada iz 2019. godine na *Binance*, jednu od najvećih mjenjačnica kriptovaluta, je prouzročio štetu od 7047 bitcoinova što je u to vrijeme iznosilo više od 40 milijuna dolara. Mjenjačnica je nakon pokušaja napada u ožujku 2018., u kojem su napadači pokušali ukrasti identitete korisnika krađom korisničkih vjerodajnica putem lažne internet stranice, radi zaštite svojih korisnika od mogućih budućih napada uspostavila fond sigurnih sredstava za korisnike (eng. *Secure Asset Fond for Users* - SAFU). Od srpnja 2018. u fond se uplaćuje 10% transakcijskih naknada kako bi mogli kompenzirati gubitci korisnika, a svi gubici u napadu iz 2019. godine bili su pokriveni iz ovog fonda. Napadači su u dobro organiziranom napadu ukrali 7000 bitcoina iz Binanceovog novčanika putem jedne transakcije [31]. Napadači su koristili razne tehnike napada, tehniku *phishinga* i računanih virusa kako bi se domogli ključeva korisničkoga API-ja, tokena za dvofaktorsku autentifikaciju i drugih osobnih korisničkih podatka koje su iskoristili za infiltriranje u mrežu tvrtke u svrhu izvršenja napada. Mjenjačnica *Binance* je unatoč uspješno izvršenom napadu i dalje operativna.

Organizacije zbog različitih razloga nisu sklone objavljivati načine na koje su njihovi sustavi kompromitirani. Smatramo da opisivanje načina izvršenja napada, nakon implementiranih kontrola u sustavima i procesima, doprinosi budućem sprječavanju sličnih napada. Navedeni primjeri napada su u oba slučaja bili uspješna, ali dok je u prvom primjeru mjenjačnica bankrotirala, u drugom primjeru mjenjačnica je i dalje operativna budući da je uspješno upravljala rizikom. Neminovno je da su sve mjenjačnice ciljevi napada i da je pitanje dana kada će neka od njih biti napadnuta, ali uspostavljanjem sustava upravljanja rizikom potencijalni gubici su nadoknadivi. Unatoč tome što mjenjačnice kriptovalutama ne podliježu centralnim regulativnim tijelima, u njihovom interesu je da koriste sigurnosne standarde koje ta tijela nalažu financijskim institucijama pod njihovim nadzorom. Neki od propisa kibernetičke sigurnosti koji se primjenjuju u financijskim institucijama su:

- GDPR
- ISO/IEC 27001
- NIST
- PCI DSS
- BSA

- PSD 2
- OSFI Self Assessments.

4.3.2 DeFi napad

Decentralizirane financije (DeFi) uključuju korištenje aplikacija lanca blokova kako bi se u ekosustavu financijskih usluga otklonila potreba za posrednikom, trećom stranom. Prema nekim analitičarima, DeFi će imati veliki utjecaj na bankarski sektor budući da njihovo poslovanje uvelike ovisi o posredničkim naknadama koje naplaćuju za posredničke usluge. DeFi eliminira naknade koje banke i druge financijske institucije naplaćuju za korištenje svojih usluga. Korisnik drži svoj novac u digitalnom novčaniku i u svakom trenutku mogu doći do svojih sredstava i raspolagati njima. DeFi proširuje upotrebu lanca blokova s jednostavnog prijenosa financijskih sredstava na složenije financijske upotrebe. S DeFi-jem je često promovirana ideja „otvorenih financija".

Većina decentraliziranih financijskih aplikacija koristi Ethereum platformu budući da Ethereum platforma, u odnosu na Bitcoin platformu, daje mogućnost provedbu složenijih transakcija pomoću pametnih ugovora. Samim tim ju je lakše implementirati i koristiti za izradu drugih vrsta decentraliziranih aplikacija izvan jednostavnih transakcija. Pametni ugovori automatski izvršavaju transakciju ako su ispunjeni određeni uvjeti. Na primjer, recimo da korisnik želi da njegov novac bude poslan drugom korisniku sljedeći petak, ali samo ako se temperatura na području grada Rijeke popne iznad 10 stupnjeva Celzijusa prema DHMZ-u. Takva pravila se mogu napisati u pametnom ugovoru, a s pametnim ugovorom u korijenu, deseci DeFi aplikacija rade na Ethereum platformi.

Korištenjem DeFi-ja transakcija se obavlja točka-točka (P2P), što je jedna od temeljnih premisa DeFi-ja. Dvije strane se dogovaraju da zamijene kriptovalutu za robu ili uslugu bez uključenja posrednika. Ukoliko jedan od korisnika DeFi aplikacije ima potrebu za zajmom, isti može tražiti putem aplikacije gdje će ga algoritam pomoću pametnog ugovora upariti s korisnikom koji izdaje zajam.

Prednosti DeFi-ja su:

- decentralizirana aplikacija koja korisniku daje mogućnost prijenosa sredstava u realnom vremenu bez posredničke naknade

- mogućnost zarade
- visoka razina sigurnosti.

Nedostatci DeFi-ja su sljedeći:

- složeno korištenje
- visok rizik od prijevara.

Do zadnjeg kvartala 2022. godine, ukupna vrijednost imovine zaključena korištenjem DeFi protokola iznosila je 53,73 milijarde dolara [32]. Iznos koji je ukraden iskorištavanjem ranjivosti DeFi protokola tijekom istog razdoblja generirao je gubitak od gotovo 2,32 milijarde dolara što je porast od gotovo 50% u odnosu na 2021. godinu. Ovi iznosi su jako privlačni potencijalnim napadačima, više od 4% vrijednosti ukupnih transakcija je izgubljeno napadima na DeFi protokol.

Načini na koji napadač može iskoristiti ranjivosti DeFi-ja prije svega proizlaze iz prirode otvorenog koda. Dok s jedne strane priroda otvorenog koda osigurava transparentnost, ona s druge strane pruža mogućnost napadačima da prouče i iskoriste ranjivosti protokola. Drugi problem pri implementaciji DeFi protokola je brzina implementacije i vremenski okvir u kojem se aplikacija izrađuje. Tempo kojim DeFi projekti završavaju i izlaze u javnost ne daje mogućnost programerima za implementaciju sigurnosnih rješenja i testiranja. Često se ignoriraju ranjivosti i pogreške u cilju završetka projekta i izdavanje proizvoda prije konkurenata. Napadači mogu iskoristiti ranjivosti i dobiti pristup imovini DeFi korisnika.

Metode DeFi napada:

- Oracle manipulacija – napadač može manipuliranjem podacima ostvariti imovinsku korist.
- Logičke pogreške u pametnom ugovoru – zbog tempa implementacije rješenja na tržište, programerima često promaknu trivijalne ranjivosti i pogreške. Budući da je DeFi protokol otvorenog koda, napadač može vidjeti kod pametnog ugovora i detektirati propuste koje može iskoristiti.
- Napadi ponovnog ulaska – ovakav napad sadrži ugovor koji poziva vanjski ugovor.

Oracle manipulacija je jedan od najčešćih napada u DeFi ekosustav gdje napadač manipulira vrijednostima imovine na decentraliziranim mjenjačnicama (DEX). Ako se mjenjačnica na kojoj je cijena kompromitirana uzima kao jedini izvor cijene od strane DeFi aplikacije, napadač može kupiti imovinu ispod cijene ili prodati istu iznad poštene tržišne cijene. Budući da ova vrsta napada zahtijeva veliki kapital kako bi se ostvarila zarada, napadi na ranjive ugovore koji dopuštaju pristup velikom kapitalu po niskoj cijeni su sve učestaliji.

Kako bi DeFi ekosustav funkcionirao, uzimaju se cijene s decentraliziranih mjenjačnica (DEX) koje se koriste u pametnim ugovorima. Prilikom kreiranja aplikacije, programer jednostavno isprogramira u kodu da pametni ugovor postavi upit jednoj od mjenjačnica koja vraća povratnu vrijednost kovanice. Ako se ekosustav oslanja na podatke samo s jedne mjenjačnice, bilo koja promjena u podacima cijene u toj mjenjačnici, pametni ugovor podatak smatraju istinitim i točnim, bez obzira na istinitost podatka. Stoga ako napadač može manipulirati cijenom imovine u jednoj mjenjačnici, netočni podaci se raspršе po svim DeFi aplikacijama koje koriste podatke iz te mjenjačnice.

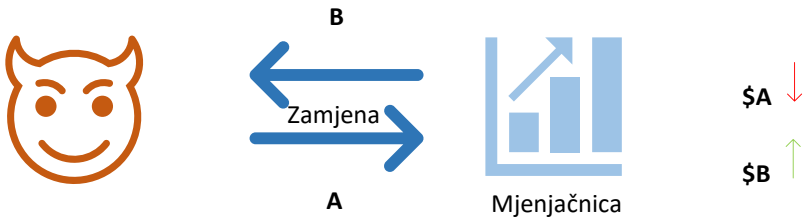
Kako funkcionira kreditiranje u decentraliziranom sustavu? U klasičnom bankarskom sustavu, za procjenu kreditne sposobnosti uzima se imovina koju zajmoprimac posjeduje, a koja služi kao osiguranje, depozit. Iznos kredita proporcionalno ovisi o imovini zajmoprimca koja se procjenjuje od strane zajmodavca. Sličan proces se događa i kod kreditiranja u decentraliziranom sustavu, osim što ulogu zajmodavca mijenja pametni ugovor. Depozit zajmoprimca čine kriptokovanice, a kako bi se dobila fer vrijednost kovanica koje zajmoprimac posjeduje, pametni ugovor postavlja upit mjenjačnici o trenutnoj vrijednosti valute koju zajmoprimac posjeduje. U slučaju da zajmoprimac ima mogućnost da manipulira podacima u mjenjačnici, može povisiti svoj depozit na osnovi kojega može dobiti veći zajam.

Novi zamah kod kreditiranja u decentraliziranim sustavima čine zajmovi bez osiguranja, zajmovi koji ne zahtijevaju depozit. Brzi zajmovi u decentraliziranom sustavu često su meta napada zlonamjernih napadača. U nastavku su opisani koraci za napad na DeFi ekosustav manipulacijom cijene kovanica u mjenjačnicama brzim zajmovima [33].

1.

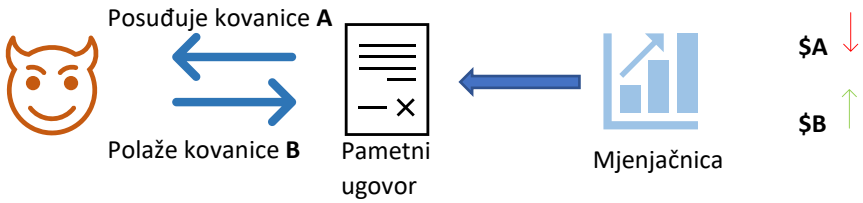
Napadač uzima brzi zajam kovanice A iz ekosustava koji podržava brze zajmove.

2.



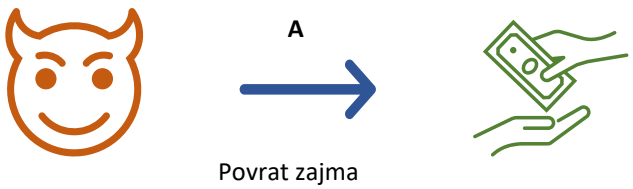
Napadač radi zamjenu kovanica A kovanicom B čime snižava cijenu kovanice A u mjenjačnici dok cijena kovanice B raste

3.



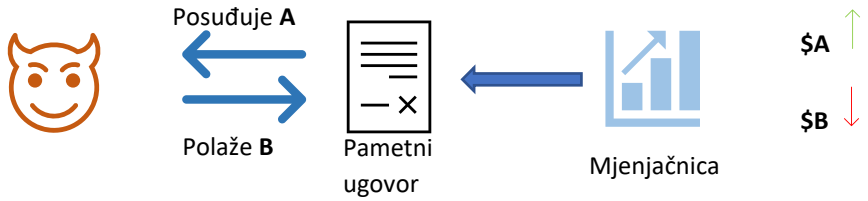
Napadač polaže kupljene kovanice B kao depozit, a radi uzimanja novog zajma kovanice A iz decentraliziranog sustava koji koristi mjenjačnicu iz koraka 2. kao izvor cijena. U koraku 2. manipuliralo se cijenom kovanica A, a zajmovi kovanica A bi trebali biti onemogućeni.

4.



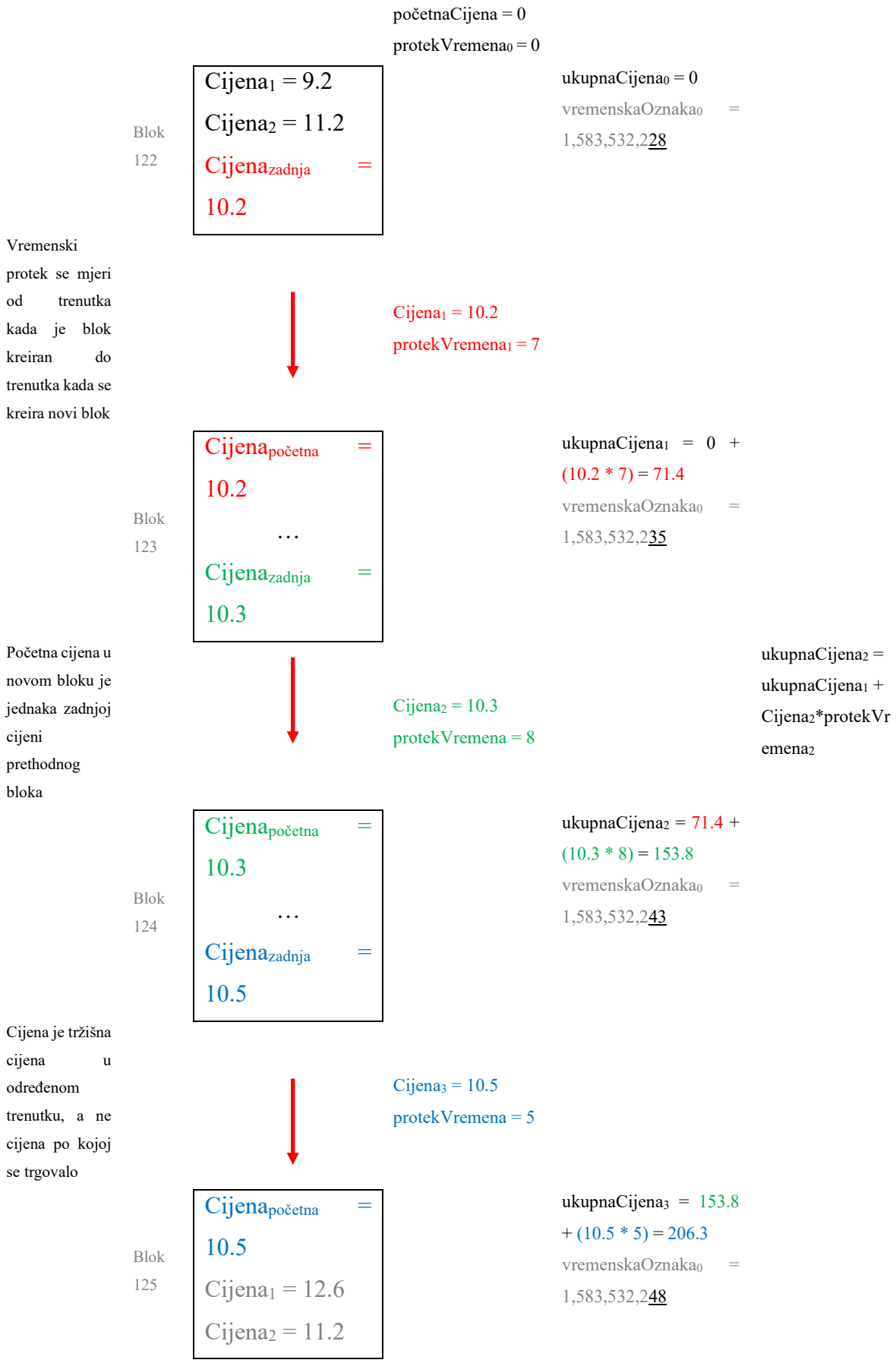
Napadač vraća zajam iz koraka 1. zajmom kovanica A uzetih u koraku 3. te zadržava preostale kovanice generirajući dobit manipulirajući cijenom u koraku 2.

5.

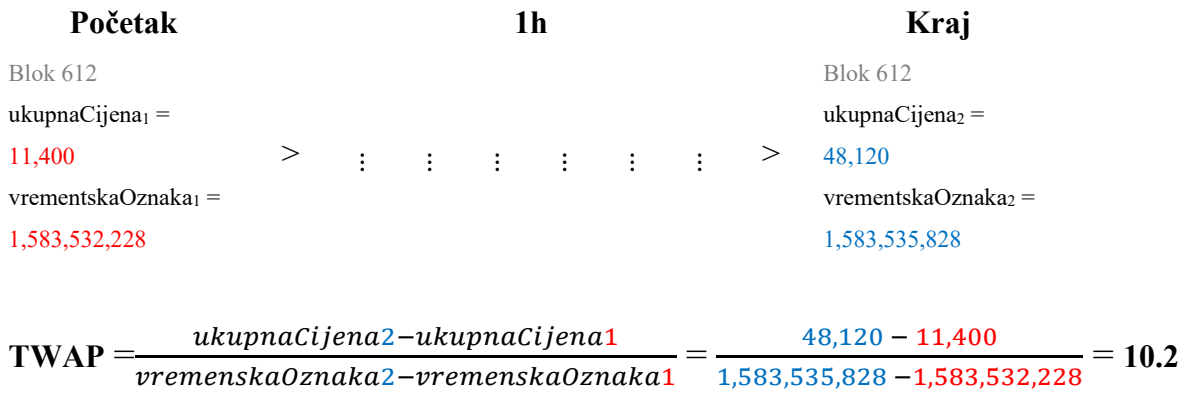


Cijena kovanice A se na tržištu vraća na fer vrijednost čime je napadač manipulacijom cijena ostvario neopravdanu dobit, dok su korisnici decentraliziranog sustava koji daju zajmove izravno oštećeni čime je smanjena likvidnost decentraliziranog sustava.

Iz prethodnog primjera napadaču je omogućena brza zarada na račun brzih zajmova što mu omogućava decentralizirani sustav, a na štetu korisnika koji daju zajmove. Razlog zbog kojeg je došlo do ovakvog rezultata je činjenica da je decentralizirani sustav iz kojeg je uzet zajam koristio jednu mjenjačnicu kao izvor tržišne cijene. Kako bi se izbjegle ovakve i slične manipulacije cijenom, umjesto da se cijene zapisuju u blok, tržišna vrijednost će se zapisivati prije početka trgovine na početku svakog bloka. Budući da je cijena unaprijed definirana i zapisana u prethodnom bloku, njome je teže manipulirati (slika 4.2.). Kako bi im to bilo moguće, potrebno je da manipuliraju cijenom iz prethodnog bloka na način da postignu konsenzus u mreži, što je malo vjerojatno i iznimno teško. Osim toga, posljednja cijena svakog bloka će se zbrojiti kako bi se dobila vremenski ponderirana prosječna cijena (eng. *time-weighted average price* - TWAP) za bilo koji željeni vremenski interval (slika 4.3.) [34].



Slika 4.2. *Pohrana kumulativnih podataka o cijenama u lancu blokova*



Slika 4.3. *Vremenski ponderirana prosječna cijena*

4.3.3 51% napad

Ako napadač posjeduje veliku količinu kovanica, može iskoristiti mehanizam protokola upravljanja i ostvariti dodatnu zaradu. To je poznato kao napad 51% i može se kombiniranjem brzog zajma kreirati napad bez posjedovanja kovanica u vlasništvu. Vidjeli smo iz primjera DeFi napada da korisnik u slučaju da ima više od 50% vlasništva kovanica A može ostvariti konsenzus koji njemu ide u prilog. Naprimjer, napadač može brzim zajmom posuditi 51% kovanica A (ili posuditi novac da kupi kovanice A), zatim izraditi i odobriti prijedlog za slanje 100 milijuna dolara stabilnih kovanica sebi. Na kraju on treba samo vratiti zajam koji je uzeo i ostaje mu zarada od 100 milijuna dolara u stabilnim kovanicama. Stabilna kovanica je kriptovaluta koja veže vlastitu tržišnu vrijednost za vanjsku „stabilnu“ pričuvnu imovinu poput zlata ili fiat valute (npr. američki dolar) [35].

Dana 17. travnja 2022. na projektu *Beanstalk Farms* dogodila se eksplozija brzih zajmova. *Beanstalk Farm* je projekt decentraliziranog financiranja (DeFi) čiji je cilj uravnotežiti ponudu i potražnju imovine kriptovalute. Napadač je iskoristio Beanstalkov sustav upravljanja većinskim udjelom, iznad 50%, koja je temeljna značajka mnogih DeFi protokola [36]. Napadač je koristio brze zajmove kako bi povećao iznos kovanica u svom vlasništvu čime bi si omogućio kontroliranje rezultata konsenzusa te se na taj način domogao sredstava na mreži. Izgubljeno je 182 milijuna dolara, a napadač je ostvario zaradu od 76 milijuna dolara. *Beanstalk* se reklamira kao decentralizirani protokol stabilne kovanice, bean, temeljen na kreditiranju. Vrijednost jedne kovanice vrijedi približno 1,00 američkih dolara. Prema analizi sigurnosne

tvrtke *CertiK*, napadač na *Beanstalk* farmu iskoristio je brzi zajam dobiven putem decentraliziranog protokola, *Aave*, kako bi posudio gotovo milijardu dolara denominiranih u različitim stabilnim kovanicama te ih zamijenio za dovoljno bean kovanica što mu je omogućilo 67% udjela. Cijeli proces uzimanja zajma je trajao manje od 13 sekundi. Inače, *Aave* je decentralizirani sustav za posuđivanje, brze zajmove, koji korisnicima omogućuju da uzmu zajam, daju zajam i zarađuju na kamatama na kriptoimovini bez posrednika. Deponiranje bean kovanica u Beanstalk mrežu, napadaču je omogućilo stvaranje zlonamjernog prijedloga „InitBip18“. Taj prijedlog, BIP, je omogućio prijenos sredstava nakon što je proteklo 24 sata od prijedloga pozivanjem „hitnog postupka“ u ugovora, a za koji se koristi `emergencyCommit()` funkcije u kodu [37].

```
function emergencyCommit(unit32 bip) external
{
     require(isNominated(bip), „Governace: Not nominated.„);
     require(Block.timestamp >=
timestamp(bip).add(C.getGovernanceEmergencyPeriod()),
„Governance: Too early.“);
     require(isActive(bip), „Governance: Ended.“);
     require(bipVotePercent(bip).greaterThanOrEqualTo(C.getGo
vernanceEmergencyThreshold()),“Governance: Must have super
majoriti.“);
     _execute(msg.sender, bip, false, true);
}
```

Kako bi se izvršio prijedlog `emergencyCommit()` funkcija, napadač mora zaobići nekoliko validacija:

Validacija 1: `require(isNominated(bip)` provjerava da li je BIP pokrenut i ne izvršen.

Validacija 2: radi se provjera je li proteklo 24 sata od predlaganja BIP-a.

Validacija 3: provjerava se je li BIP aktivan.

Validacija 4: postotak za izvršavanje „hitnog postupka“ prema BIP-u ne smije biti manji od praga, a koji iznosi 2/3.

Napadači su čekali da protekne 24 sata nakon čega su pozvali „hitni postupak“. Kako su pomoću brzog zajma osigurali sebi više od 78% glasova, što je više od potrebnih 67%, zlonamjerni prijedlog „InitBip18“ je prošao.

Napadači su zatim vratili zajam ostvarujući neto zaradu od 76,2 milijuna dolara denominiran u ethereum kriptovaluti. Pomoću servisa *Tornardo Cash,* u nizu od 270 transakcija, uspjeli su sakriti tragove žetona i oprati ukradena sredstva, a iznos od 250 000 američkih dolara stabilnih kovanica su donirali za pomoć Ukrajini.

Nakon napada, bean kovanica koja je u biti stabilni kovanica i vezana uz američki dolar u omjeru 1:1, je pala za 78,3% i trgovalo se po 0,21 američkih dolara. Ulagačima u projekt *Beanstalk* izgubljena sredstva nisu nadoknađena i prema izjavama osnivača *Beanstalka* malo je vjerojatno da će ikada biti obeštećeni.

Ovaj napad je izvršen u proljeće 2022. kombiniranjem ranjivosti DeFi protokola i ranjivosti od 51% glasova. Nova tehnologija donosi nove ranjivosti koju napadači pokušavaju iskoristiti, a tehnologija lanca blokova daje mogućnost napadačima da prikriju svoje tragove. Potpuna transparentnost koju nam omogućuje tehnologija lanca blokova daje nam mogućnost da promatramo i proučavamo napade nakon što se dogode. Također nam olakšava procjenu financijskog učinka napad što je uvijek izazovno.

4.3.4 Phishing napad

Danas se svakodnevno spominju prednosti kriptovalute i sigurnost koju nam pruža u usporedbi s drugim načinima digitalnog plaćanja. Do sada smo vidjeli da korištenje tehnologije lanca blokova ima mnoge prednosti u pogledu kibernetičke sigurnosti, ali ne štiti korisnika od mogućih prijevara. Svakodnevni rast prijetnji, poput *phishing* napada putem leda (eng. *ice phishing*), naglašava ranjivosti bez obzira na korištenje tehnologije lanca blokova.

Kako bismo mogli razumjeti *ice phishing,* potrebno je razumjeti pozadinu Web3 koncepta. Web3 je decentralizirani svijet u kojem se koriste najnapredniji kriptografski sigurnosni mehanizmi koristeći tehnologiju lanca blokova. Sredstva koja su pohranjena u digitalnom novčaniku bez skrbništva su osigurana privatnim ključem dok su pametni ugovori

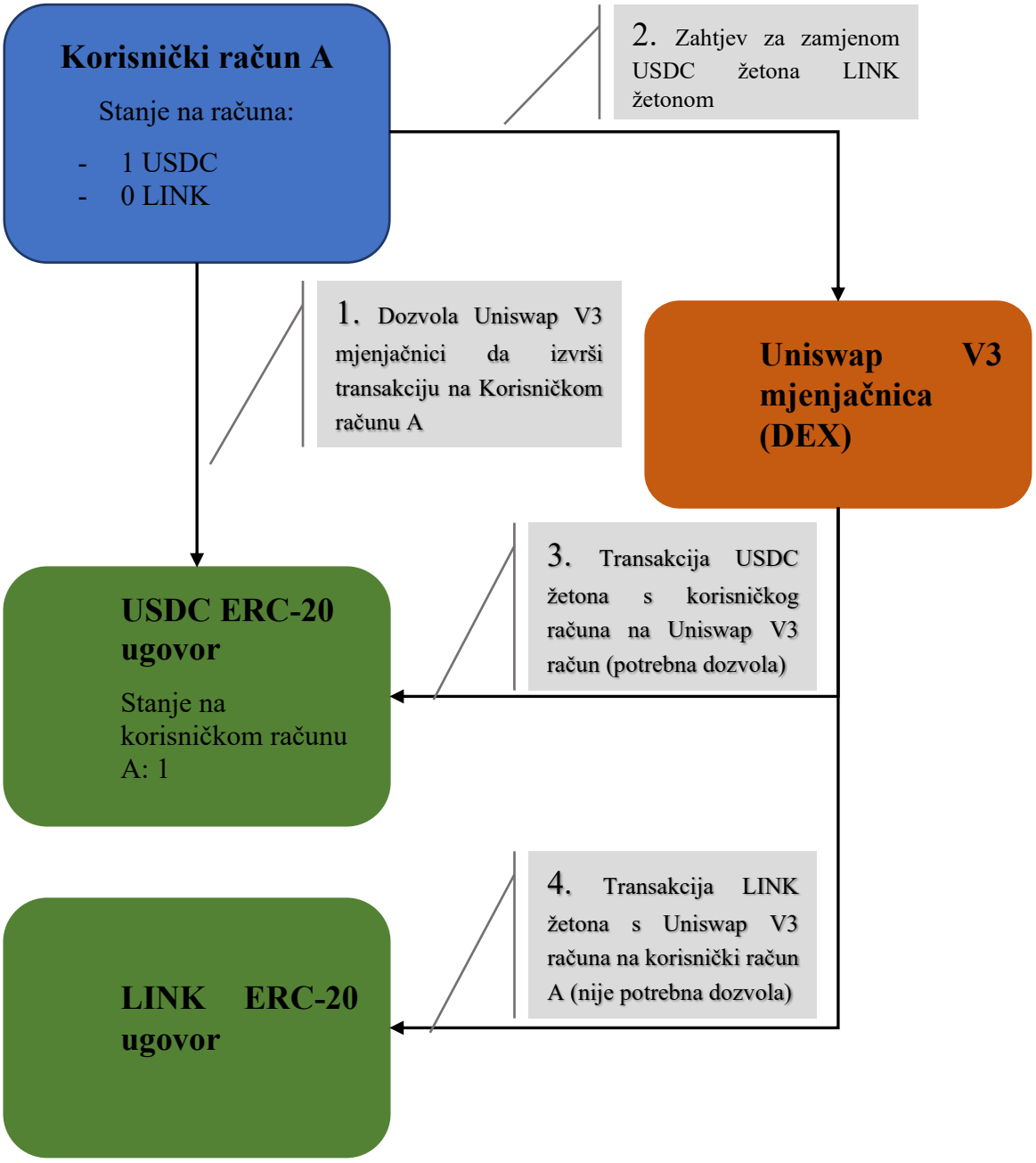
nepromjenjivi. S obzirom na sigurne temelje, možemo se zapitati kako se događaju *phishing* napadi. Lanac blokova je distribuirana knjiga zaštićena kriptografskim algoritmima. Najveći lanci blokova su trenutno bitcoin i ethereum. Lanac blokova se može zamisliti kao baza podataka koja prikazuje prijenos kovanica kriptovaluta s jednog računa na drugi. Računi su povezani s kovanicama kriptovalute dok novčanici vizualiziraju kovanice kriptovalute povezane s našim računima. Novčanici ne drže naše kriptovalute, već su kovanice pohranjene u distribuiranu knjigu, odnosno lanac blokova. Novčanik nam omogućava korištenje kriptografskih ključeva za potpisivanje transakcija koje se obavljaju na kovanicama kriptovalute povezane s našim računom. Naši kriptografski ključevi omogućavaju nam pristup našim kovanicama kriptovalute. Krađa ovog ključa daje mogućnost napadaču da prebaci sredstva bez našeg pristanaka. Postoje dvije vrste novčanika, skrbnički i neskrbnički. Dok su skrbnički povezani s mjenjačnicama kriptovaluta, neskrbnički novčanici se nalaze na našem uređaju i pružaju nam mogućnost pristupa kriptografskim ključevima. Radi razumijevanja *ice phishing* napada potrebno je upoznati ERC-20 žetone. Radi se o posebnim kovanicama kriptovalute, žetona, koji se implementiraju putem ERC-20 pametnog ugovora. Za prijenos žetona s jednog računa na drugi, pošiljatelj kao vlasnik mora odobriti prijenos. Vlasnik žetona može dati odobrenje dodatnim entitetima, poput pametnih ugovora, da automatski obavljaju prijenos sredstava u ime korisnika. To je posebno bitno u decentraliziranim financijama (DeFi), poput decentralizirane mjenjačnice (DEX), radi razmjene žetona različitih kriptovaluta.

Tradicionalni *phishing* napadi u Web2 svijetu usmjereni su na krađu vjerodajnica korisničkih računa usmjeravanjem korisnika na nelegitimne web stranice, naprimjer zlonamjerna web stranica identična web stranici naše banke. Ekvivalent vjerodajnicama u Web2 svijetu su naši šifrirani privatni ključevi pohranjeni u našim digitalnim novčanicima [38]. Tehnike slanja masovnih poruka putem elektroničke pošte koju su napadači koristili kako bi se domogli naših vjerodajnica je teško primjenjiva kada je cilj napada naš privatni ključ, a zbog male vjerojatnosti da će poruka stići u pretinac korisnika kriptokovanica. Zbog toga se koriste različite metode kako bi se došlo do korisnika kriptovalute i pokušalo na prijevaru doći do privatnog ključa:

- Na društvenim mrežama platformi za kriptovalute se prate korisnici koji se obraćaju korisničkoj podršci te im se zlonamjerni napadači naknadno izravno obraćaju u ime podrške, a u cilju krađe privatnog ključa [39].
- Besplatno slanje novih kovanica skupini korisnika (npr. *Airdrop* kovanica), a zatim slanje poruke o neuspješnoj transakciji uz slanje linka na web stranicu koja služi za krađu identiteta [40].

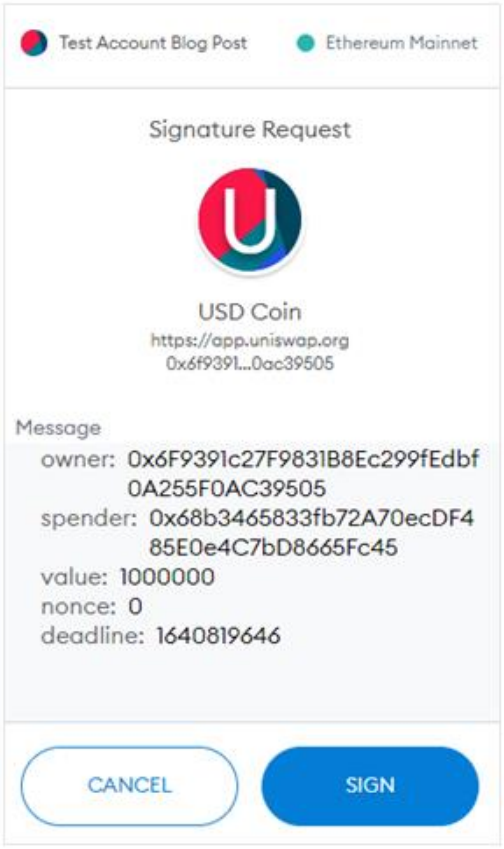
- Preusmjeravanje na web stranicu s koje se skida dodatak za aplikaciju koja se koristi za rudarenje na vlastitom uređaju, a u cilju krađe vjerodajnica s našeg uređaja [41].
- Prevaranti skupljaju krivo napisane URL nazive kriptovaluta kako bi predstavljali legitimne kriptovalute (naprimjer, conibase.com umjesto coinbase.com ili www.cripto.com umjesto www.crypto.com) [42].
- Lažni softverski novčanik i izravna krađa privatnih ključeva.

Tehnika *ice phishinga* ne uključuje krađu privatnih ključeva već podrazumijeva prijevaru korisnika da potpiše transakciju koja skida sredstva sa našeg računa na račun napadača. Na slici 4.4. prikazano je kako izgleda tijek transakcije koja uključuje DeFi pametni ugovor u procesu zamjene kovanica. Za svaku transakciju potrebno je odobrenje što je ujedno i prvi korak. Nakon što je odobrenje odobreno, pametnom ugovoru se dopušta prijenos USDC kovanica, u ime korisnika, radi zamjene LINK žetonima. Ovdje nailazimo na problem Web3 aplikacije. Naime, korisnik ne može jednostavno poslati potrebnu količinu kovanica na adresu pametnog ugovora aplikacije već umjesto toga aplikacija traži odobrenje zahtjeva od strane korisnika za kasnije povlačenje kovanica u ime korisnika (korak 3). U praksi, mnoge aplikacije zahtijevaju odobrenje praktički za neograničene količine kovanica umjesto da traže odobrenje samo za potrebnu količinu. To se često radi kako bi se smanjili transakcijski troškovi, pa je „zahtjev za neograničenim kovanicama“ postao industrijska praksa.



Slika 4.4. *Tijek transakcije u procesu zamjene žetona*

Kako bi mogli objasniti način na koji napadač može izvesti napad je potrebno da poznajemo značenje adresa u transakciji. Adresa predstavlja pametni ugovor ili novčanik i zapisana je u heksadecimalnom obliku od 42 znaka. U prethodnom primjeru, transakcija kao odredišnu adresu sadrži ERC-20 pametni ugovor, a da bi napadač uspješno izveo *ice phishing* napad, potrebno je da zamijeni odredišnu adresu adresom novčanika koju kontrolira napadač (slika 4.5.) [43].



Slika 4.5. *Zahtjev za potpisom odobrenja transakcije*

Izvor: Halborn.com [43]

Ako promotrimo prethodnu sliku, vidimo da zahtjev za odobrenje transakcije sadrži izvorišnu i odredišnu adrese u heksadecimalnom zapisu. Dok je izvorišna adresa (eng. *owner*), adresa našeg novčanika, problem predstavlja nedovoljno informacija o odredišnoj adresi (eng. *spender*), 0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45. Radi li se o legitimnoj adresi ili adresi koju kontrolira napadač, teško je procijeniti budući da ne vidimo sve relevantne podatke koji nam mogu pomoći da uvidimo da je zahtjev za transakcijom izmijenjen.

Jednom kada je transakcija odobrena, u slučaju da je napadač kompromitirao transakciju i zamijenio adrese, napadač može isprazniti novčanik žrtve. Upravo to se dogodilo prilikom napada na *BadgerDAO* kada su napadači uspjeli ukrasti 120 milijuna američkih dolara u nekoliko minuta. *BadgerDAO* je decentralizirana autonomna organizacija koja koristi DeFi protokol kako bi pružila mogućnost korisnicima da ostvaruju kamate na bitcoin depozite.

Korisnici deponiraju bitcoin kovanice u trezore koji se koriste za daljnja ulaganja. Način na koji su napadači izveli napad je da su ubacili zlonamjerni *javascript* kod na web stranicu aplikacije Badger. Prema nekim informacijama je navodno Cloudflareov račun *Badger* projekta, koji je sadržavao API, bio kompromitiran [44]. Zlonamjerni kod je generirao lažna odobrenja transakcija koja su slana korisnicima. Odobrena transakcija od strane korisnika je omogućilo napadačima da u budućnosti povuku sredstva u svoje vlastite novčanike umjesto u one koje kontrolira *BadgerDAO*. Napadači su potiho skupljali odobrenja tijekom studenog 2021. godine kako bi prikupili što veći broj odobrenja. 1. prosinca 2021. jedan od korisnika s 50 milijuna američkih dolara vrijednim kovanicama na računu je dao odobrenje, što je potaklo napadače da aktiviraju povlačenje te su u roku od 6 sati povukli sva sredstva korisnika koji je imao 50 milijuna američkih dolara na računu kao i sredstva s računa ostalih korisnika koji su dali odobrenje. Ukupna je ukradeno 120 milijuna američkih dolara s računa korisnika [45].

Budući da su transakcije na mrežama lanca blokova javne, to nam daje mogućnost prepoznavanja ovakvih i sličnih napada u ranoj fazi i automatizirano djelovanje u smislu obustavljanja budućih transakcija. Danas su nam dostupne platforme koje analiziraju aktivne pametne ugovore i mogućnost otkrivanja prijetnji u stvarnom vremenu. Postoji niz preporuka koje bi korisnik trebao poduzeti kako bi izbjegao da postane žrtva, ali nedostatak svih tih preporuka je potrebna količina znanja krajnjeg korisnika. Sve aplikacije imaju za cilj prikupiti što više korisnika pa su tako izdane preporuke korisnicima u velikoj mjeri većini korisnika nejasne. Umjesto da se korisnicima daju preporuke da provjeravaju je li pametni ugovor izmijenjen ili ima li pametni ugovor ugrađene mehanizme odgovora na incident poput pauziranja transakcija, trebalo bi krajnjem korisniku omogućiti jednostavniju vizualnu provjeru. Na davateljima usluge je da rade provjere ugovora, izvršavaju sigurnosne provjere svojih web stranica pa i u krajnjoj mjeri osigurati fond iz kojeg bi se nadoknađivala šteta prouzročena kibernetičkim napadima.

4.3.5 Ransomware

Korištenje tehnologije lanca blokova nije izravno povezano s *ransomware* napadima već se neizravno koristi kako bi napadač mogao doći do materijalne koristi. *Ransomware* je zlonamjerni softver koji korisnicima onemogućuje pristup sustavu ili podacima, zahtijevajući

od korisnika otkupninu kako bi ponovno dobili pristup. Na različite načine *ransomware* može zaraziti korisničko računalo:

- *malspam*, slanje zlonamjernog softvera putem elektroničke pošte,
- *malvertising*, slanje zlonamjernog softvera putem mrežnog oglašavanja,
- *spear phishing*, slanje zlonamjernog softvera putem elektroničke pošte ciljanoj skupini korisnika,
- društveni inženjering.

Koju god metodu napadač koristi kako bi dobio pristup računalu, jednom aktiviran softver za ucjenjivanje šifrira korisničke dokumente tako da mu korisnik ne može pristupiti zahtijevajući plaćanje otkupnine kako bi vratili ono što su oduzeli. U sljedećem koraku u prvi plan dolazi tehnologija lanca blokova. Naime, napadači, kako bi prikrili tragove novca, zahtijevaju da se otkupnina plati putem kriptovalute. Prvi *ransomware* napadi datiraju još iz 1989. godine, a pojava bitcoina i drugih kriptovaluta, rezultirala je naglim porastom *ransomware* napada. Razlog leži u tom da su pojavom kriptovalute napadači dobili mogućnost iznude velikog iznosa novca, a pritom ostaju anonimni i teško im je ući u trag. Loša je vijest da kriminalne skupine koje se bave kibernetičkim napadima ulažu napore da automatiziraju proces prodaje *ransomwarea*, a prvi korak ka unapređenju *ransomware* napada je kreiranje platforme *ransomeare-as-a-service* (RaaS). Ovakve platforme daju mogućnost svojim klijentima, napadačima, da prilagode mnoge aspekte zlonamjernog programa, uključujući vektore napada, metodu šifriranja, ciljane datoteke i poruke. Sljedeći korak je uporaba tehnologije lanca blokova kako bi unaprijedili RaaS platformu. Na primjer, napadač bi mogao sklopiti pametni ugovor prema kojem bi programer *ransomwarea* dobio proviziju samo u slučaju da je *ransomware* učinkovit. Tako napisan ugovor na lancu blokova je nepromjenjiv za bilo koju stranu.

Prema nekim istraživanjima, samo četvrtina žrtava *ransomwarea* uspije u potpunosti vratiti svoje podatke nakon plaćanja otkupnine [46]. Ujedno su se pojavili napadači koji, nakon što bi primili otkupninu, ne bi poslali ključeve za dešifriranje podatka ili bi nastavili s daljnjom ucjenom i prijetnjom kako će objaviti podatke do kojih su došli tijekom napada. To je doprinijelo da je žrtva izgubila povjerenje u napadača kao osobu koja može otključati šifrirane podatke. Korištenjem tehnologije lanca blokova, napadači mogu razmjere napada podići na višu razinu kako bi stekli povjerenje žrtve i povećali vjerojatnost za plaćanje otkupnine po principu dešifriranje po skupini podataka, primjerice dešifriranje samo slika. Plaćanje otkupnine po dešifriranje, koju napadačima omogućava tehnologija lanca blokova, je nova paradigma koju

istraživači proučavaju. U osnovi, poluautonomni *ransomware* temeljen na lancu blokova bi koristio pametne ugovore koji bi ujedno žrtvi bili jamstvo da će dobiti pristup podacima u slučaju da plate otkupninu [47]. Ukoliko bi podaci nakon plaćanja otkupnine i dalje bili šifrirani, pametni ugovor bi stopirao isplatu sredstva napadaču. Iz ovoga možemo vidjeti da i napadači žele uvesti reda u područje *ransomware* napada. Danas su ovakvi napadi postali sofisticiraniji te su rezultat pojedinaca i organizacija koja su razvila poslovanje na *ransomware* napadima. Smatramo da će podizanje ovakvih napada na višu razinu, uvođenje tehnologije lanca blokova u njihovo izvođenje, popularizirati izvođenje napada, a žrtve će biti sklonije plaćanju otkupnine. Također će izvođenje ovakvih napada postati društveno prihvaćeno budući da će napadači sami nastojati uvesti etična načela. Djelovanje po principu „ako ti ne vratim podatke nećeš platiti“ o napadačima daje dojam poslovnih osoba, dok će žrtva postati zadovoljan ili nezadovoljan kupac.

Ako tehnologiju lanca blokova primijenimo na strani žrtve, možemo preventivno djelovati u obrani od *ransomware* napada. Problem žrtve kod *ransomware* napada, zbog čega su oni i uspješni, su podaci koji nisu adekvatno zaštićeni i nemaju sigurnosnu kopiju. Ako pak žrtva pohrani svoje podatke u distribuiranu knjigu, takvi zapisi se raspoređuju po više poslužitelja, decentralizirani su, umjesto da su pohranjeni na jednom centralnom mjestu. Ukoliko napadač uspješno izvede napad na jednom poslužitelju, žrtva uspješno može doći do svojih podataka povratom kopija na drugim poslužiteljima. Lanac blokova nam na ovaj način osigurava dostupnost nepromjenjivih podataka bez oslanjanja na središnji entitet.

4.3.6 Zamjena SIM-a

Ova vrsta napada je sljedeći korak koji slijedi nakon napada društvenim inženjeringom. Cilj napadača je prebaciti telefonski broj žrtve na SIM karticu, fizičku ili virtualnu, pod kontrolom napadača. Obično cilja na ranjivosti prisutnoj u 2FA, dvofaktorskoj autentifikaciji, gdje je drugi korak za potvrdu pristupa unos koda primljenog putem SMS poruke. Na ruku napadačima ide činjenica da većina telekoma daje svojim pretplatnicima mogućnost da prebacivanje broja s jedne SIM kartice na drugu obave putem korisničke službe. Napadači su danas sve domišljatiji i uvjerljiviji, a agenti u korisničkoj službi su često slabo educirani i pod pritiskom da zadovolje korisnika. Ovi koraci se obično primjenjuju nakon što je pravi vlasnik broja izgubio telefon ili mu je ukraden. Nerijetko se događa da napadači angažiraju osobu

unutar telekoma koja će surađivati i omogućiti im prebacivanje broja vlasnika na SIM karticu u vlasništvu napadača. U tim trenucima na telefonu pravog vlasnika usluga će biti nedostupna i vjerojatno neće ni posumnjati o čemu se radi. Meta ovih napada su u velikoj mjeri vlasnici kriptomjenjačnica i veliki investitori u kriptovalute.

Načini na koji se može napraviti zamjena SIM kartice su sljedeći:

1. Da bi se napad uspješno izveo, potrebno je doći do privatnih podataka osobe koja je meta napada što se najčešće izvodi društvenim inženjeringom. Primjer: „ *Dobar dan, danas sam izgubio telefon i imam hitni slučaj zbog kojem moram prenijeti svoj broj na novi telefon. Prilično mi je hitno jer očekujem vrlo važan poziv. Pripremio sam broj osobne iskaznice i kućnu adresu.*“

   Danas smo svjedoci da se broj osobne iskaznice ostavlja na svakom koraku, a nerijetko se događa da se njezina kopija ostavlja osobama za koje nismo sigurni čuvaju li podatke u skladu sa zakonom o zaštiti podataka. Podaci koji se traže putem telefonskog razgovora s agentom su upravo podaci s osobne iskaznice, broj osobne iskaznice i adresa.
2. Putem *phishing* napada ili putem klasične provale u računalo poslovnog subjekata koji unutar trgovačkog centra prodaje telekom usluge. Nerijetko se ovi prostori nalaze unutar trgovačkih centara bez fizičke zaštite od prolaznika. Također, iako subjekt ne radi, računala mogu biti fizički dostupna što daje mogućnost napadaču da ih zarazi zlonamjernim softverom kako bi mogao napraviti zamjenu SIM kartica.
3. Zaposlenik telekoma može surađivati s napadačima ili sam prodavati uslugu SIM zamjene.

Iz prethodno nabrojanih primjera kako se može napraviti zamjena SIM-a, možemo zaključiti da je napad zamjenom SIM-a jedna od jednostavnijih metoda napada. Budući da je ovaj napad lako izvesti, često su način napada mladih i neiskusnih napadača zbog čega često budu i uhvaćeni. Prilikom izvođenja ovakvih napada često ostaju tragovi zbog kojih je lako locirati mjesta s kojih je napad izveden. U rujnu 2018. godine, napadači su zamjenom SIM-a zaposlenika *Crowd Machine* ukrali 14 milijuna dolara. *Crowd Machine* je startup koji se bavio kriptovalutama te je ubrzo nakon napada objavio da je pristup njihovom novčaniku ugrožen i da su kovanice iz novčanika ukradene. Objavili su i adresu novčanika na koju su napadači prebacili sredstva, 0x290d615eE921706ec8cCB2593F09B2D2e0F8B67c. Prema policijskom izvještaju, napadači su prebacili žrtvin broj telefona na uređaj koji se nalazi u blizini hotela

SpringHill Suites, 510 S. MacArthu Blvd, Oklahoma City. Policija je otkrila da su napadači kupili mobitel u obližnjem WalMartu gdje su snimljeni nadzornom kamerom pomoću kojih su identificirani. Jedan od napadača je kupio mobitel 18. rujna dok je drugi napadač unajmio sobu 17. rujna, a odjavio 25. rujna [48].

U SAD-u su žrtve „zamjena SIM kartica" podigle tužbe protiv *AT&T* i *T-Mobile*. Odvjetnički tim koji vodi postupak protiv telekoma u ima žrtava navode da telekomi snose svoju odgovornost optužujući ih da su sigurnosne procedure koje telekomi provode pune propusta. Također, navode da su slabom edukacijom svojih zaposlenika doprinijeli tome da su lopovi uspješno radili zamjene SIM kartica putem telefonskih poziva, pristupa financijskim podacima i informacijama o računima žrtva te pražnjenju računa kriptovaluta i druge vrijedne imovine [49].

4.3.7 Lažni novčanik

Sigurna pohrana kriptovaluta ili drugih informacija u lanac blokova je nešto što nam je zajamčeno korištenjem tehnologije lanca blokova. Ali da bismo pohranili podatke u lanac blokova, potrebna nam je aplikacija koja nam pruža takvu mogućnost, pomoću koje možemo pristupiti našem računu, obavljati transakcije i provjeravati stanje našeg računa.

Ako koristimo kriptovalute, nikada nećemo imati priliku držati tu istu kriptovalutu u rukama, ne postoji fizička kovanica ili novčanica koju možemo vidjeti. Kada obavljamo kupnju kriptovalutom, ista je šifrirana i zapisana u lancu blokova. Ono s čime zapravo radimo kada koristimo kriptovalutu su javni i privatni ključevi kojima kontroliramo sredstva, imovinu. A upravo je najbitnije te ključeve pohraniti i čuvati na sigurnom jer bez njih nećemo moći pristupiti našoj imovini. Na primjeru upravljanja sredstvima na bankovnom računu napravit će se primjer kako funkcionira upravljanje računom koji koristi tehnologiju lanca blokova. Javni ključ za našu kriptoimovinu ima isto značenje kao i broj našeg bankovnog računa. Javni ključ je informacija koju dijelimo prilikom transakcije. Privatni ključ ima značenje poput PIN-a, daje pristup sredstvima. Dakle, ukoliko zlonamjerni korisnik dođe do našeg javnog ključa i privatnog ključa, on zapravo ima kontrolu nad našim kriptosredstvima. Kako bi korisnik čuvao privatni i javni ključ na sigurnom mjestu, najbolje mjesto za to su kripto ili digitalni novčanik. Digitalni novčanik dolazi u dvije vrste, softverski i hardverski.

Softverski novčanik može se podijeliti u tri vrste [50]:

- mrežni novčanik,
- desktop novčanik i
- mobilni novčanik.

Mrežni novčanik je zapravo web aplikacija, imovina koju posjedujemo je pohranjena na web mjestu entiteta preko kojeg smo izvršili transakciju, primjerice kriptomjenjačnica. Ovi novčanici su besplatni, a sredstva kojima raspolažemo su nam odmah dostupna. Sigurnost web novčanika na prvom mjestu ovisi o nama, a zatim o entitetu na kojem se nalazi novčanik. U cilju svakog entiteta koji se bavi kriptoimovinom je da implementira sigurnosne mehanizme u cilju sprječavanja krađe sredstava korisnika, ali isto tako, budući da ne postoje regulatorna tijela koja nadgledaju takve entitete, nitko ne može jamčiti da su implementirana u skladu s preporukama i najboljom praksom. Stoga čuvanje ključeva na web mjestima predstavlja opasnost od krađe uzrokovane napadima odlučnih hakera. Prepuštanje čuvanja javnih i privatnih ključeva trećim stranama, poput mjenjačnice koju koristimo za trgovanje kriptovalutama, nije preporučljivo.

Desktop novčanici su sigurnija opcija, ako ih usporedimo s mrežnim novčanicima, pa su samim time i bolja opcija. Korištenjem desktop novčanika osigurali smo da nitko osim nas samih nema pristup digitalnoj imovini

Mobilni novčanici su mobilne aplikacije koje se koriste na Android, iOS ili Windows mobilnim uređajima tako da pored što sami čuvamo digitalna sredstva, ista su nam dostupna u svakom trenutku jer im se može pristupiti s bilo kojeg mjesta. Mobilni novčanici nisu najsigurnija rješenja s obzirom na veliki rizik od krađe ili gubitka mobilnog uređaja.

Krajem 2022. godine u Googleovoj platformi za distribuciju digitalnog sadržaja*, Play trgovina*, nalazilo se 2.68 milijuna aplikacija [51] dok se u Appleovoj platformi za distribuciju digitalnog sadržaja, *Apple trgovina*, u istom razdoblju nalazilo 1.64 milijuna mobilnih aplikacija [52]. Prije nego aplikacija postane dostupna u trgovini, obje kompanije ulažu trud u mehanizme i kontrole kako bi spriječili da zlonamjerna aplikacija uđe u trgovinu i postane lako dostupna svima. Samim time je i broj zlonamjernih mobilnih novčanika koji se pronalaze u mobilnim trgovinama u stalnom porastu. Napadači imaju jednostavnu računicu, izrada zlonamjerne mobilne aplikacije i njezino ubacivanje u trgovinu aplikacija ima trošak od nekoliko tisuća eura. Ako samo jedan korisnik te aplikacije postane ujedno i žrtva, napadač može lako ostvariti zaradu. Krajnjim korisnicima je jako teško ocijeniti koja je aplikacija „prava“, a koja je „lažna“. Danas su napadači organizirani i ne predstavlja im nikakav problem izraditi aplikaciju i web

stranicu profesionalno i identičnu originalnoj. Čak je i ocjenu aplikacije u trgovini, a koju korisnici često koriste kao podatak i informaciju na temelju koje prosuđuju je li aplikacija lažna ili prava, lako lažirati. U konačnici je vrlo teško krajnjem korisniku utvrditi pouzdanost mobilne aplikacije, pa tako i kada se radi o mobilnom novčaniku. Aplikacije koje izrađuju velike kompanije se trude na svaki negativni komentar odgovoriti što nam može biti jedna od informacija koju provjeravamo prilikom preuzimanja aplikacije.

Hardverski digitalni novčanik je fizički uređaj koji pohranjuje našu kriptoimovinu. Prilikom povezivanja hardverskog novčanika s računalom putem USB priključka, od korisnika će se tražiti da unese PIN kod [50]. Za razliku od softverskih novčanika koji su povezani s internetom i smatraju se ranjivim, hardverski novčanik se smatra sigurnijim rješenjem. Budući da hardverski ključevi nisu povezani s internetom, napadači ne mogu pristupiti privatnim ključevima koji su pohranjeni na njemu. Prilikom potpisivanja transakcije, korisnik mora priključiti hardverski ključ na računalo kako bi odobrio i dovršio transakciju.

Krajem 2018. godine dvojca prijatelja su zaboravila znamenke PIN-a Trezora hardverskog novčanika na kojem su imali pohranjeni privatni ključ kojim su mogli pristupiti kriptokovanicama u protuvrijednosti od nekoliko milijuna dolara. Pokušali su pogoditi PIN upisujući 4-znamenkasti broj, ali nakon desetog pokušaja su odustali jer bi nakon šesnaest neuspješnih pokušaja podaci na ključu bili trajno obrisani. Istraživanjem po internetu i u prepiskama po forumima stupili su u kontakt s hardverskim hakerom Joeom Grandom, poznat po hakerskom imenu „Kingpin“. Inače, Grand je široj javnosti bio poznat kao dio skupine *L0pht* koja je 1998. svjedočila u američkom Senatu o ranjivostima koje bi se mogle koristiti za rušenje interneta i presretanje prometa [53]. Nakon razgovora s Grandom, prijatelji su bili uvjereni da će im njegove vještine omogući da dođu do izgubljenog PIN-a hardverskog ključa. Grand je korištenje ranjivosti hardverskog ključa otkrivene 2017. smatrao previše riskantnim da bi ih primijenio u ovom slučaju. Naime, britanski haker, Saleem Rashid, je otkrio da Trezorov hardverski novčanik, prilikom ažuriranja *firmware*a, premješta PIN i privatni ključ iz sigurne *flash* memorije u RAM memoriju. Problem je što se nenamjernim brisanjem RAM memorije, a prije nego se pročitaju podaci, trajno gubi mogućnost pristup hardverskom ključu. Ipak, na tragu te metode, Grand je naišao na bolje rješenje. Otkrio je da verzija *firmwarea* hardverskog ključa u njegovom slučaju, kopira privatni ključ i PIN u RAM, a ne da premješta. Izvođenjem napada na čip ključa, promjenom napona na mikrokontroleru, razina sigurnosti na mikrokontroleru se smanjuje s RDP2, najsigurnije razine koja ne dopušta čitanje RAM memorije, na sigurnosnu razine RDP1, razinu koja dopušta čitanje RAM memorije. Budući da

su PIN i privatni ključ samo kopirani iz *flash* memorije u RAM memoriju, nije postojala opasnost od gubitka trajnog pristupa hardverskom novčaniku. Bilo je potrebno samo generirati pravu razinu napona na mikrokontroleru koja bi smanjila razinu sigurnosti mikrokontrolera što mu je u konačnici uspjelo nakon 4 sata [54].

Prethodni primjer je dokaz da u slučaju gubitka hardverskog novčanika naša imovina u lancu blokova nije sigurna. Ako usporedimo s razinom sigurnosti koju nam pruža softverski novčanik, u obliku mobilne aplikacije kao najzastupljenijim rješenjem digitalnog novčanika, hardverski novčanik pruže daleko veću razinu sigurnosti. Problem kod digitalnih novčanika u obliku mobilne aplikacije je mogućnost njezinog kopiranja od strane napadača. Korisnici digitalnih trgovina na Android i iOS sustavima su skloni bezuvjetno vjerovati aplikacijama koje se pronalaze u njima. Napadači su svjesni toga i pokušavaju iskoristiti korisničku nepažnju plasirajući zlonamjernu aplikaciju u digitalne trgovine. To se i dogodilo Phillipe Christodoulou koji je, u želji da ima konstantni pristup svojem računu s kriptosredstvima, skinuo aplikaciju Trezor iz *Apple trgovine* na svom mobilnom uređaju. Inače, *Apple* slovi za proizvođača koji „kontrolirala najpouzdaniju trgovinu aplikacija na svijetu“, koji ne objavljuje aplikacije u svojoj trgovini bez sigurnosne provjere svake od njih i proizvođač uređaja na kojem se ne mogu instalirati aplikacije iz nepoznatih izvora. S druge strane, Trezor je proizvođač hardverskih novčanika i ime Trezor, zaštitni znak aplikacije koji je bio identičan korištenom logu proizvođača hardverskih novčanika i visoke ocjene aplikacije u trgovini, bile dovoljne informacije korisniku da ocijeni ovu aplikaciju kao pouzdanu i instalira ju na svom mobilnom uređaju. Prilikom prvog korištenja aplikacije od korisnika se tražilo da upiše svoj PIN i frazu koju korisnik koristi u slučaju gubitka PIN broja. To su bile dovoljne informacije kojima je napadač prebacio sredstva u svoj kriptonovčanik. Sigurno se pitamo kako je moguće da se pored svih sigurnosnih kontrola koje *Apple*, prema njihovim riječima, provodi prilikom provjere svake aplikacije, zlonamjerna aplikacija nalazila u njihovoj digitalnoj trgovini. Napadači su prije svega uspjeli dovesti u zabludu *Apple* prilikom provjere aplikacije Trezor. Naime, programeri zlonamjerne aplikacije Trezor su unatoč tome što je koristila Trezor ime, logo i boje, aplikaciju prema *Appleu* predstavili kao aplikaciju koja bi šifrirala datoteke na iOS mobilnim uređajima i služila za sigurnu pohranu lozinki na uređajima. Također je navedeno od strane programera aplikacije da se aplikacije neće koristiti ni u jednom pogledu za trgovanje kriptovalutama. *Apple* je dana 23. siječnja 2021. odobrio aplikaciju i postavio u *Apple trgovinu*. Nakon toga, bez saznanja *Applea*, program je aplikaciju za šifriranje Trezor promijenio u digitalni novčanik. Sam *Apple* takve promjene ne dopušta, ali isto tako nije ih u mogućnosti

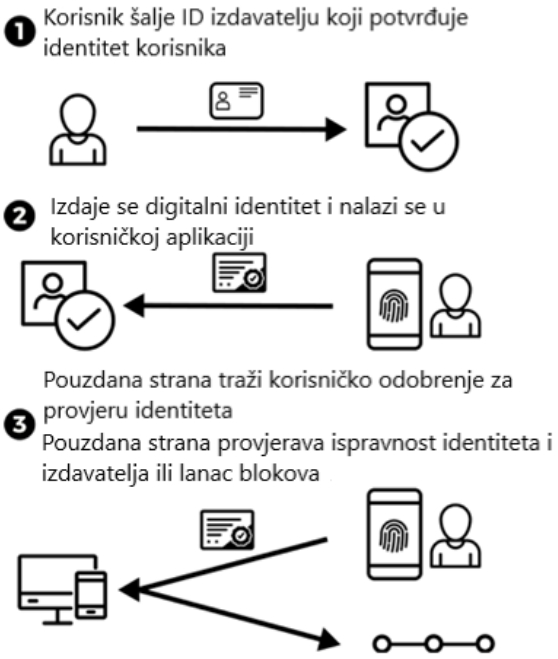
spriječiti niti se može znati kada će se dogoditi. Nakon što je tvrtka *Trezor* prijavila lažnu aplikaciju u digitalnoj trgovini, *Apple* ju je uklonio i blokirao programera. Prema izvještaju tvrtke *Sensor Tower*, zlonamjerna aplikacija Trezor je bila u *Apple trgovini* najmanje od 23. siječnja 2021. do 3. veljače 2021. te je imala oko 1000 preuzimanja [55]. Korisnici Trezorovih hardverskih novčanika su dovedeni u zabludu da je aplikacija Trezor aplikacija koja će im omogućiti provjeru stanja svoje kriptoimovine pohranjene u hardverskom novčaniku. Nakon što bi korisnici unijeli PIN, aplikacija se nikad ne bi „povezala“ s njihovim hardverskim novčanicima pa bi jednostavno zaključili kako aplikacija ne radi. Tek bi prilikom sljedećeg pristupa hardverskim novčanicima vidjeli da su im nestala sredstva, a s foruma bi saznali da mobilna aplikacija Trezor, proizvođača hardverskih novčanika Trezor, nikada nije postojala. Pet osoba je prijavilo da im je lažna aplikacija Trezor, skinuta iz *Apple trgovine*, ukrala kriptoimovinu u vrijednosti od 1,6 milijuna američkih dolara, dok su tri osobe prijavila da im je aplikacija Trezor, instalirana na Android uređajima, ukrala kriptoimovinu u vrijednosti od 600.000 američkih dolara.

Iz spomenutih primjera napada na digitalne novčanike možemo zaključiti da ni jedan oblik pohrane podataka nije u potpunosti siguran bez obzira na korištenje tehnologije lanca blokova. Korištenje tehnologije lanca blokova podiže razinu sigurnosti na višu razinu, ali isto tako dovodi u zabludu korisnike da je njihova imovina pohranjena u lancu blokova sigurna. Također, subjekti koji koriste tehnologiju lanca blokova za svoje mrežne servise, zbog nepostojanja centralnog tijela koje će nadzirati njihov rad, nisu nadzirani niti su primorani provoditi sigurnosne kontrole. U početku su, kada je lanac blokova bio u povojima, nastupali samouvjereno da su neprobojna tvrđava u kojoj su sredstva korisnika sigurno pohranjena. Danas se takav pristup mijenja i uvode sigurnosne kontrole, ali bez regulativnih tijela koja bi trebala nadzirati rad takvih subjekata sredstva korisnika nisu osigurana.

4.3.8 Napad na digitalnu vozačku dozvolu

Krajem 2019. godine vlada Novog Južnog Walesa u Australiji je uvela digitalne vozačke dozvole (eng. *Digital Driver License* – DDL). Digitalne vozačke dozvole omogućile su stanovnicima koji ih posjeduju da svoj identitet i dob dokazuju pomoću svojih pametnih telefona. Digitalne vozačke dozvole su, prema riječima vlade pružala, dodatnu razinu sigurnosti i zaštitu od prijevare identiteta u usporedbi s plastičnim vozačkim dozvolama. Nije dugo trebalo

da se dokaže suprotno, da se trivijalnim tehnikama krivotvori identitet na digitalnim vozačkim dozvolama. Kako izgleda proces izdavanja digitalnog identiteta prikazano je na slici 4.6.



Slika 4.6. *Okvir povjerenja temeljen na lancu blokova*

Kako izgleda sustav digitalnog identiteta? Sustav digitalnog identiteta je digitalna mreža koju čine pružatelj usluge digitalnog identiteta, korisnik koji koristi tu uslugu i subjekt u čijem je interesu provjera identiteta korisnika radi pružanja svojih usluga (naprimjer, banke, telekomi, policija prilikom provjere, itd.). Podaci se ne čuvaju u središnjoj bazi već su decentralizirani. Prilikom prvog koraka stvaranja digitalnog identiteta, korisnici se prijavljuju na platformu za provjeru identiteta, izdanu od državnog tijela, kako bi stvorili i registrirali digitalni identitet. Tijekom procesa stvaranja digitalnog identiteta, korisnik stvara par privatnih i javnih ključeva. Javni ključevi povezani s digitalnim identitetom se mogu pohraniti u lancu blokova, u slučaju da su ključevi ugroženi ili zbog rotacije ključeva, iz sigurnosnih razloga. Ono što je ključno je da podaci o osobi ne bi trebali biti pohranjeni u lanac blokova radi skalabilnosti i kako bi bili u skladu sa zakonima o privatnosti. Digitalni identitet omogućuje korisnicima sustava lakši, brži i sigurniji pristup podacima, ali na sljedećem primjeru ćemo vidjeti kako je moguće manipulirati podacima o osobi baš zato što podaci nisu zapisani u lanac blokova već na uređaj korisnika.

Ako se vratimo na primjer digitalne vozačke dozvole države Novi Južni Wales, subjekti koji žele provjeriti identitet osobe skeniraju QR kod koji se nalazi na uređaju korisnika. Ako je korisnik manipulirao s podacima na svom uređaju, žrtva neće znati da su podaci neistiniti. DDL (slika 4.7.) zahtijeva iOS ili Android aplikaciju koja prikazuje vjerodajnice svake osobe.

Slika 4.7. *Digitalna vozačka dozvola države Novi Južni Wales*

Izvor: [56]

Ista aplikacija omogućuje subjektima koji rade provjeru identiteta provjeru na temelju autentičnosti vjerodajnice. Značajke koje se nalaze na digitalnoj vozačkoj dozvoli su sljedeće [56]:

1. animacija loga države Novi Južni Wales
2. datum i vrijeme zadnjeg ažuriranja podataka
3. QR kod
4. hologram u pozadini koji se pomiče kako se telefon naginje

5. vodeni žig koji odgovara fotografiji koja se nalazi na DDL
6. adresa osobe.

Prilikom otvaranja aplikacije koja sadrži DDL, potrebno je unijeti 4-znamenkasti PIN. Ključ napada upravo leži u tehnici napada uzastopnim pokušajima, odnosno grubom silom, nad 4-znamenkastim PIN-om. Budući da PIN sadrži samo 4 znamenke, postoji samo 10 000 mogućih kombinacija. Korištenjem javno dostupnih skripti te standardnim računalom, moguće je otkriti PIN u svega nekoliko minuta. Jednom kada je dostupan pristup šifriranim podacima koji se nalaze na digitalnoj vozačkoj dozvoli, tehnikom napada grubom silom moguće je pročitati i izmijeniti podatke. Koraci za napad na DDL koji se nalazi na IPhone uređaju su sljedeći [57]:

1. Appleovim alatom za izradu sigurnosne kopije, *iTunes*, potrebno je napraviti sigurnosnu kopiju sadržaja telefona, iPhone uređaja, spremajuću vjerodajnice koje napadač želi izmijeniti,
2. izdvojiti šifrirane datoteke iz sigurnosne kopije kreirane u prvom koraku,
3. koristiti softver za napade grubom silom kako bi se dešifrirale datoteke,
4. otvoriti datoteku u uređivaču teksta i promijeniti datum rođenja, adresu ili druge podatke koje se želi lažirati
5. ponovno šifrirati datoteku
6. šifriranu datoteku kopirati u sigurnosnu kopiju napravljenu u prvom koraku
7. vratiti sigurnosnu kopiju na iPhone.

Nakon što se sigurnosna kopija vrati na pametni uređaj, DDL će prikazati podatke koji su izmijenjeni u koraku 4. Iz ovoga primjera možemo vidjeti da izvođenjem jednostavnih tehnika napada možemo izmijeniti podatke u nečemu što smatramo sigurnim jer je novo, digitalno i koristi tehniku lanca blokova. Svaki sustav ima dvije strane, korisničku stranu i servisnu stranu. Ulaganjem resursa u zaštitu samo jedne strane, a ne mareći za sigurnost druge strane, narušava se cijeli sustav.

Različiti propusti u dizajnu sustava omogućili su ovakve sigurnosne propuste nad DDL-om, a koje je moguće iskoristiti primjenom jednostavnih vektora napada. Prvi sigurnosni propust je neodgovarajuća zaštita prilikom provjere identiteta, odnosno korištena metoda provjere identiteta 4-znamenkastim PIN-om je krajnje neadekvatna. Drugi sigurnosni propust, odnosno veliki nedostatak je da se podaci s DDL-a nikada ne provjeravaju pozadinskim sustavom. Ovdje možemo već reći da je ova mana rezultat pobijanja tehnologije lanca blokova i zakona o privatnosti. Tehnologija lanca blokova ne dopušta brisanje podatka, dok s druge strane zakon o

privatnosti nalaže da privatni podaci na zahtjev korisnika moraju biti izbrisani. Bez mogućnosti provjere ispravnosti podataka, ne postoji način da se utvrdi da je došlo do neovlaštenog mijenjanja podataka. Treći nedostatak je što se prilikom ažuriranja QR koda ne osvježavaju pohranjeni podaci. Posljednji nedostatak je postojanje mogućnosti sigurnosnog kopiranja i vraćanja podataka. Naime, iOS sustav ima mogućnost da se prilikom izrade sigurnosnog kopiranja izuzmu određene datoteke što su, zbog sigurnosnih razloga, programeri trebali koristiti prilikom dizajniranja i izrade sustava.

5. Vrste rizika kod primjene tehnologije lanca blokova

Danas se smatra da je tehnologija lanca blokova druga era interneta. Tehnologija lanca blokova, ako izuzmemo korištenje u području kriptovaluta, će iz temelja transformirati poslovni svijet baš kao što je internet napravio revoluciju u dijeljenju informacija i trgovini. Dok su zagovaratelji novih tehnologija uzbuđeni zbog uvođenja i korištenja lanca blokova te vide evolucijski potencijal tehnologije lanca blokova u modernizaciji poslovnog svijeta, postoje i oni koji pak zagovaraju oprezniji pristup u implementaciji nove tehnologije. Bez obzira na krajnji ishod brzine uvođenja lanca blokova u sustave, neminovno je da će se u budućnosti revizori suočiti s brojnim pitanjima i odlukama u vezi s procjenom rizika svojstvenih tehnologiji lanca blokova. Revizori moraju biti spremni procijeniti te rizike i njihov potencijalni financijski učinak kao i mogući učinak na integritet cjelokupnog poslovanja.

Lanac blokova, iz revizorskog kuta gledanja, pokriva temeljne sigurnosne kriterije informacijske sigurnosti. Prvo, korištenje javnih i privatnih ključeva za osiguranje podataka koristi najsuvremeniju kriptografiju. Drugo, sustav je distribuiran i decentraliziran što nam pruža rasprostranjenost baze podataka na više računala. Treće, lančano povezivanje nepromjenjivih blokova, koje sadrže informacije, stvara savršenu revizijsku povijest. Cjelovitost informacija u lancu blokova osigurana je kombinacijom javnih i privatnih ključeva, a kod provjere sudjeluje većina računala na mreži.

Unatoč svim prednostima koje tehnologija lanca blokova pruža, lanac blokova, kao i svaka nova tehnologija, ima brojne inherentne rizike. Ovi rizici uključuju [58]:

- operativne i IT rizike,
- rizike sigurnosti podataka,
- regulatorne rizike,
- rizike treće strane,
- rizike privatnosti.

5.1 Operativni i IT rizici

Tehnologija lanca blokova zahtijeva značajne računalne i energijske resurse za obradu velike količine transakcija što je vrlo skupo. Mali broj računala s velikom snagom u mreži lanca blokova ima veći utjecaj na konsenzus nego jednak broj slabijih računala što utječe na algoritam konsenzusa te treba razmotriti prilikom procjene rizika. Potrebno je razumjeti sve implikacije koje veliki broj računalnih sustava ili čvorova sa sobom donosi, a pogotovo danas kada se radi uštede energije računalni sustavi nalaze u stranim zemljama gdje je električna energija jeftinija. Potrebno je voditi računa o potrebnim resursima koje tehnologija lanca blokova zahtijeva, kako energijski tako i ljudskim resursima.

Lanac blokova je složeni sustav i dio je šire tehnološke infrastrukture. Svakodnevnim tehnološkim napretkom te napretkom kvantnog računarstva i kriptografije brzo bi mogli zastarjeti najsuvremeniji sustavi. S druge strane dizajniranje sustava temeljenog na lancu blokova mora se često integrirati s naslijeđenim sustavima i sustavima trećih strana kao i s drugim lancima blokova. Prilikom pristupa korištenju tehnologije lanca blokova, organizacije moraju razmotriti sve tehnološke rizike koje takvi sustavi donose. Potrebno je uspostaviti kontrole koje osiguravaju opsežno testiranje svih aspekata integracije lanca blokova.

5.2 Rizici sigurnosti podatka

Većina organizacija poduzima značajne korake kako bi osigurale sigurnost podataka. U lancu blokova, postoji ljudski element koji se koristi prilikom unosa i prilikom pronalaženja podatka, a koji se oslanja na kriptografsku zaštitu javnih i privatnih ključeva kako bi osigurao sigurnost podataka. To znači da posjedovanje ključeva i vlasništvo nad podacima postaju jedno. Ako ključevi padnu u pogrešne ruke, integritet unesenih podataka i pristup podacima je ugrožen. Javni i privatni ključevi su ključni za integritet informacija u lancu blokova zbog čega je potrebno uspostaviti kontrole za sprječavanje neovlaštenih osoba u pristupu javnim i privatnim ključevima. Također treba voditi računa da se koriste sigurne metode šifriranja ključeva, a računala koja se koriste za unos ključeva moraju biti zaštićena antivirusnim softverom.

Pametni ugovori su ono što poslovni sustav temeljen na lancu blokova čini naprednijim od postojećih poslovnih sustava. Pametni ugovori omogućavaju programiranje pravne, ekonomske ili poslovne logike unutar poslovnog sustava radi automatizacije poslovnog procesa što ih čini metom broj jedan za napadača. Kako bi se pametni ugovor izvršavali u skladu s poslovnim procesom, prije implementacije je potrebno provesti odgovarajuća testiranja.

5.3 Regulatorni rizik

Entiteti koji sudjeluju u lancu blokova nisu ograničeni državnim granicama niti su regulirani regulatornim i zakonskim propisima. Međutim, postoje entiteti, organizacije i pojedinci koji sudjeluju u lancu blokova u skladu sa zakonima i propisima države u kojoj su registrirani za obavljanje djelatnosti. To ipak znači da korištenje lanca blokova unutar određene zemlje ili grupe zemalja neće biti u skladu s propisima i zakonima tih zemalja. Primjer za to je Opća uredba EU o zaštiti podataka. Potrebno je da entiteti poduzimaju korake kako bi njihovo sudjelovanje na određenom tržištu bilo u skladu sa zakonima i propisima te zemlje. Potrebno je također promotriti sve obveze i implikacije poslovanja u nereguliranom okruženju. Također je potrebno uspostaviti mehanizam za rješavanje razlika u okruženjima različitih regulatora. Stoga bi pametni ugovori trebali omogućiti rukovanje u iznimkama što ujedno znači veći rizik. Zato je bitno pametne ugovore testirati na više mreža, propisa i drugih ograničenja ili okuženja u kojima se moraju izvršiti.

5.4 Rizik dobavljača trećih strana

Ni jedan poslovni sustav nekog poslovnog subjekta danas nije izgrađen bez sudjelovanja trećih strana u njezinoj izgradnji. Poslovni subjekti koji koriste aplikacije ili programske module trećih strana, koji se koriste za pravilno funkcioniranje sustava temeljenog na tehnologiji lanca blokova, moraju razmotriti rizike povezane s integritetom i profesionalnošću dobavljača. Naprimjer, ako aplikacija ili modul koji je razvila treća strana ima slabosti, njezine slabosti se mogu prenijeti u slabosti lanca blokova poslovnog sustav subjekta koji ga koristi. Također, postoji velika vjerojatnost da će zaposlenici trećih strana imati pristup povjerljivim vjerodajnicama lanca blokova. Treće strane koji sudjeluju u izgradnji poslovnog sustava trebaju biti temeljito provjerene. Također je potrebno uvesti evidenciju o trećim stranama koja bi služila

radi osiguranja dugoročnog odnosa s njima. Potrebno je uspostaviti kontrole koje omogućuje kontinuirano praćenje odnosa s trećim stranama. Reference kupaca i mogućnost provjere zadovoljstva s kupcima koji su koristili usluge dobavljača mogu doprinijeti smanjenju rizika povezanim s dobavljačima trećih strana.

5.5 Rizik privatnosti

Po samoj svojoj prirodi, javni lanac blokova je otvoren svima. To znači da svi sudionici mogu vidjeti informacije i transakcije unesene u distribuiranu knjigu. Neki od tih podatka mogu biti povjerljivi ili vrlo osjetljivi. Stoga, prije prelaska na ekosustav lanca blokova, potrebno je biti upoznat s rizicima privatnosti. Kako bi se smanjio rizik neovlaštenog pristupa privatnim i osjetljivim podacima, potrebno je uspostaviti kontrole za ograničavanje pristupa podacima samo ovlaštenim sudionicima. Također je potrebno kreirati politiku privatnosti, koja bi pokrivala prikupljanje, korištenje i sigurnost osobnih podataka, dovoljno čvrstu da djeluje u ekosustavu lanca blokova.

6. Procjena rizika tehnologije lanca blokova

Procjena rizika je jedan od osnovnih elemenata sustava upravljanja rizikom svake organizacije. U nastavku će se napraviti kvalitativna analiza rizika tehnologije lanca blokova primjenom NIST SP-800-30 metodologije. Cilj procjene rizika tehnologije lanca blokova je predočiti korisnicima i arhitektima poslovnih rješenja, temeljenima na tehnologiji lanca blokova, moguće rizike u primjeni ove tehnologije. U procjeni će biti navedene kontrole i protumjere kako bi se lanac blokova učinio sigurnijim prilikom implementacije i korištenja.

Prijetnje i ranjivosti koje su promatrane kod procjene rizika su temelji napada obrađenih u ovom radu. Tako u primjeru DeFi napada, potencijalna ranjivost u pametnom ugovoru je temelj za DeFi napad.

6.1 Čimbenici rizika

Čimbenici rizika su karakteristike u modelima rizika koje se koriste kao ulazne vrijednosti za određivanje rizika prilikom procjene rizika. Čimbenici rizika uključuju prijetnju, ranjivost, posljedice i vjerojatnost. U dokumentu su čimbenici rizika definirani na sljedeći način [59]:

- Prijetnja je svaka okolnost ili događaj neovlaštenog pristupa s potencijalno nepovoljnim posljedicama na sustav, s ciljem uništavanja, otkrivanja ili izmjene informacija ili uskraćivanja usluge. Izvori prijetnji mogu biti ljudska pogreška, kvarovi na sustavima, prirodne katastrofe, kvarovi izvan kontrole organizacije ili kibernetički napad.
- Ranjivost je slabost sigurnosnih politika i procedura sustava, slabost u internim kontrolama ili implementaciji koju izvor prijetnji može iskoristiti.
- Vjerojatnost pojave je ponderirani čimbenik rizika koji se temelji na analizi vjerojatnosti da određena prijetnja može iskoristiti ranjivost. Čimbenik rizika vjerojatnosti kombinira procjenu vjerojatnosti da će prijetnja rezultirati štetnim posljedicama. Procjena vjerojatnosti napada obično se temelji na:
    - namjeri,
    - sposobnosti,
    - cilju.
- Razina posljedica prijetnje je veličina štete kao posljedica štetnog događaja.

Iz navedenog možemo zaključiti da je rizik vjerojatnost gubitka u slučaju štetnog događaja.

6.2 Model procjene i podaci o prijetnjama

Potrebno je identificirati pretpostavke u području prijetnje te izvor prijetnje kako bi se napravile relevantne procjene rizika za svaku prijetnju.

6.2.1 Izvor prijetnji

Kod procjene rizika tehnologije lanca blokova, kao izvor prijetnji, promatrane su isključivo prijetnje prouzročene namjernim ljudskim djelovanjem, pojedinca ili kriminalnih skupina, dok prijetnje prouzročene nenamjernim djelovanjem, poput ljudske pogreške, strukturalnih kvarova sustava ili prirodnih katastrofa, nisu razmatrane prilikom procjene.

Kako bi se bolje razumjele potencijalne ljudske prijetnje, potrebno je kategorizirati napadače koji mogu naštetiti informacijskoj imovini s obzirom na raspoložive resurse, upornost i motive. Radi boljeg pregleda procjene, napadači su podijeljeni u dvije grupe na osnovi karakteristika napadača koji se mogu pronaći u biblioteci agenata prijetnji (eng. *Threat Agent Library*)[60] (tablica 6.1.).

Tablica 6.1. *Podjela napadača i njihove karakteristike*

	Kriminalne skupine	Pojedinci
Pristup	Vanjski	Vanjski
Dostupni resursi	Visoki	Umjereni
Vještine	Visoke	Visoke

Izvor: [60]

Kriminalne skupine su vanjski napadači koji u većini slučajeva djeluju pod pokroviteljstvom vlada država, korporacija ili terorističkih organizacija. Često su sofisticirani s velikim financijskim i tehnološkim resursima na raspolaganju te posjeduju napredne tehničke vještine. Pojedinci, odnosno *hakeri*, predstavljaju vanjsku osobu koja mora, u našem slučaju, posjedovati dobre tehničke vještine te na raspolaganju imaju ograničene financijske i tehnološke resurse.

6.2.2 Potencijalne prijetnje

Podjela potencijalnih prijetnji:

- Mrežna prijetnja: Distribuirani napadi uskraćivanja usluge (DDoS), manipulacija vremenskom oznakom, *Sybil* napad, *Eclipse* napad, particioniranje, presretanje komunikacije, odgađanje,
- Prijetnja dvostruke naplate: 51% napad, *Malleability* napad, utrka napad, *Finney* napad, Vektor 76 napad, napad grubom silom,
- Prijetnja privatnom ključu: krađa novčanika, napad čovjek u sredini, ranjivost u kriptografiji,
- Prijetnja pametnom ugovoru: zlonamjerni pametni ugovor, ranjivost u pametnom ugovoru.

6.2.3 Vjerojatnost prijetnje

Vjerojatnost pojavljivanja i realiziranja prijetnji se temelji na subjektivnoj procjeni i izrađena je pomoću kalkulatora za kvantitativnu procjenu [61]. Kvantitativne vrijednosti dobiveni korištenjem spomenutog kalkulatora su mapirane u kvalitativne vrijednosti pomoću tablice 6.2.

Tablica 6.2. *Ljestvica vjerojatnost prijetnji*

Kvalitativna vrijednost	**Kvantitativna vrijednost** [61]	**Opis**
Vrlo visoka	9,0 – 10	Gotovo sigurno pokretanje prijetnji od strane napadača
Visoka	7,0 – 8,9	Velika vjerojatnost pokretanja prijetnji od strane napadača
Umjerena	4,0 – 6,9	Donekle vjerojatno pokretanje prijetnji do strane napadača
Niska	2,0 – 3,9	Mala vjerojatnost pokretanja prijetnji od strane napadača

Vrlo niska	0 – 1,9	Vrlo mala vjerojatnost pokretanja prijetnji od strane napadača

6.2.4 Posljedice prijetnje

Posljedice prijetnji određuju se na temelju izvora prijetnji, ranjivosti i implementiranih ili planiranih protumjera. Ljestvica procjene posljedica prijetnji prikazana je u tablici 6.3.

Tablica 6.3. *Ljestvica posljedica prijetnje*

Kvalitativna vrijednost	**Opis**
Vrlo visoka	Može se očekivati da će prijetnja imati katastrofalno štetne posljedice na imovinu, pojedince, organizaciju ili društvo.
Visoka	Može se očekivati da će prijetnja imati katastrofalno negativan učinak na imovinu, pojedince i samu organizaciju. Primjerice, rezultira velikim financijskim gubitkom, ostavlja veliku štetu na imovinu organizacije ili rezultira gubitkom života.
Umjerena	Prijetnja ima ozbiljan negativan učinak na organizaciju, imovinu organizacije, pojedince ili društvo. Primjerice, uzrokuje smanjenu učinkovitost organizacije, rezultira značajnim financijskim gubitkom ili prouzrokuje štetu pojedincima koja ne uključuje gubitak života ili ozljede opasne po život.
Niska	Prijetnja će imati ograničen nepovoljan učinak na organizaciju i njezinu imovinu. Rezultira manjom štetom na organizacijskoj imovini ili dovodi do manjeg financijskog gubitka.
Vrlo niska	Prijetnja ima zanemariv negativan učinak na poslovanje, reputaciju i imovinu organizacije

Izvor: [59]

6.3 Rezultat procjene rizika

Razina rizika se utvrđuje na temelju vjerojatnosti da će se prijetnja dogoditi i posljedica koje proizlazi iz navedene prijetnje. Na temelju dobivenih vrijednosti, kvalitativne vrijednosti rizika za pojedine prijetnje se dobivaju pomoću matrice u tablici 6.4.

Tablica 6.4. *Određivanje razine rizika*

Vjerojatnost (da se prijetnja dogodi i rezultira štetnim posljedicama)	**Razina posljedica**				
	Vrlo niska	**Niska**	**Umjerena**	**Visoka**	**Vrlo visoka**
Vrlo visoka	Vrlo nizak	Nizak	Umjeren	Visok	Vrlo visok
Visoka	Vrlo nizak	Nizak	Umjeren	Visok	Vrlo visok
Umjerena	Vrlo nizak	Nizak	Umjeren	Umjeren	Visok
Niska	Vrlo nizak	Nizak	Nizak	Nizak	Umjeren
Vrlo niska	Vrlo nizak	Vrlo nizak	Vrlo nizak	Nizak	Nizak

Izvor: [59]

Rezultati procjene su prikazani u tablici 6.5.

Tablica 6.5. Rezultati procjene rizika tehnologije lanca blokova

Kategorija	Prijetnja	Opis prijetnje	Izvor prijetnje	Vjerojatnost prijetnje	Posljedica prijetnje	Rizik	Kontrola
Mrežna prijetnja	Distribuirani napadi uskraćivanja usluge (DDoS)	Pokušaj sprječavanja legitimnog korištenja usluge	Skupina	Visoka	Umjerena	Umjeren	Implementacija protokola dokaz o aktivnosti, brza verifikacija, poboljšati sigurnost IoT uređaja
	Manipulacija vremenskom oznakom	Vremenska oznaka bloka mora biti veća od vremenske oznake prethodnog bloka. Manipulacijom vremena može se izbaciti čvor iz mreže.	Skupina	Umjerena	Umjerena	Umjeren	Koristiti sistemsko vrijeme čvora umjesto mrežnog vremena
	Sybil napad	Napadač kreira i kontrolira skup čvorova u cilju izvođenja drugih napada	Skupina	Umjerena	Visoka	Umjeren	Ograničavanje kreiranja više korisničkih računa, u određenom vremenskom razdoblju, s iste IP adrese

	Eclipse napad	Napadač nastoji izolirati čvor sprječavajući ga da preuzme informacije o topologiji mreže te na taj način preuzima kontrolu nad svim vezama čvora	Pojedinac	Umjerena	Visoka	Umjeren	Potreba za većim brojem veza između čvorova, otežati stvaranje novih čvorova, deterministički odabir čvorova
	Particioniranje	Nastoji se izolirati određeni čvor ili skupina čvorova. Cilj napada može biti stvaranje izdvojenog lanca, odbacivanje bloka ili poništavanje transakcija.	Skupina	Visoka	Visoka	Visok	Nadzor mreže i implementirati dostupne sigurnosne mehanizme BGP protokola
	Presretanje komunikacije	Presretanje komunikacije čvora i praćenje transakcije	Pojedinac	Umjerena	Umjeren	Umjeren	Djelomična integracija s anonimnim komunikacijskim sustavima (poput Tor mreže) smanjila bi razinu vjerojatnosti prijetnje na nisku

	Odgađanje	Napadač za cilj ima usporiti slanje informacija o novim blokovima drugim čvorovima. Može biti temelj drugim napadima.	Skupina	Visoka	Umjerena	Umjeren	Praćenje povratnog vremena (RTT) ili korištenje UDP otkucaja
Prijetnja dvostruke naplate	51% napad	Napadač kontrolira više od polovice čvorova u mreži čime upravlja konsenzusom	Skupina	Niska	Visoka	Umjeren	Slanje upozorenja o dvostrukoj naplati, postavljanje promatračkog čvora
	Malleability napad	Kod ovog napada, napadač je primatelj transakcije. Napadač modificira transakciju s ciljem da naplati obje, legalnu i modificiranu.	Pojedinac	Niska	Umjerena	Nizak	ID neovisan o potpisu
	Utrka napad	Napadač, kupac, šalje u mrežu proturječnu transakciju prije nego prodavatelj potvrdi	Pojedinac	Visoka	Umjerena	Umjeren	Postavljanje promatračkog čvora u mrežu, mjera upozorenja o dvostrukoj naplati

		legalnu, prihvaćenu, transakciju					
	Finney napad	Slično utrka napadu, napadač lažnom transakcijom poništava plaćanje dobavljaču	Pojedinac	Umjerena	Umjerena	Umjeren	Trgovci mogu u svrhu mjere opreza čekati više potvrda prije prihvaćanja plaćanja i slanja proizvoda
	Vektor 76 napad	Kombinacija utrka i *Finney* napada kako bi se poništile parne transakcije	Pojedinac	Visoka	Umjerena	Umjeren	Postavljanje promatračkog čvora u mrežu, mjera upozorenja o dvostrukoj naplati
	Napad grubom silom	Napadač kontrolira skupinu čvorova u mreži koji zajedno stvaraju alternativni lanac blokova u svrhu povrata uplate nakon dobivene usluge od trgovca	Skupina	Niska	Visoka	Nizak	Postavljanje promatračkog čvora u mrežu, mjera upozorenja o dvostrukoj naplati
Prijetnja privatnom ključu	Krađa novčanika	Do krađe novčanika dolazi zbog napada na sustav koji upravlja novčanicima, greške u	Pojedinac	Visoka	Umjerena	Umjeren	Korištenje hardverskih novčanika, implementacija PPSS-a (eng. *Password-*

		softveru ili zlonamjernog programa instaliranog na korisničkom uređaju					*Protected Secret Sharing*) i dvofaktorske autentikacija
	Čovjek u sredini	Napadač mijenja adrese primatelja transakcije, prije potpisivanja, svojom adresom	Pojedinac	Visoka	Umjerena	Umjeren	Korištenje IDS sustava
	Ranjivost u kriptografiji	Algoritmi koji se koriste u lancu blokova, ECDSA i SHA-256, pružaju jaku zaštitu, ali nisu jamac zaštite u slučaju nepravilne implementacije	Skupina	Niska	Visoka	Nizak	Specifični su za ranjivosti povezani s implementacijom stoga treba voditi računa o načinu implementiranja
Prijetnja pametnom ugovoru	Zlonamjerni pametni ugovor	Pametni ugovori se mogu koristiti za zlonamjerne aktivnosti, poput plaćanja *RaaS* usluga	Skupina	Visoka	Visoka	Visok	Implementacija sigurnosnih politika i procedura, implementacija tehničke zaštite

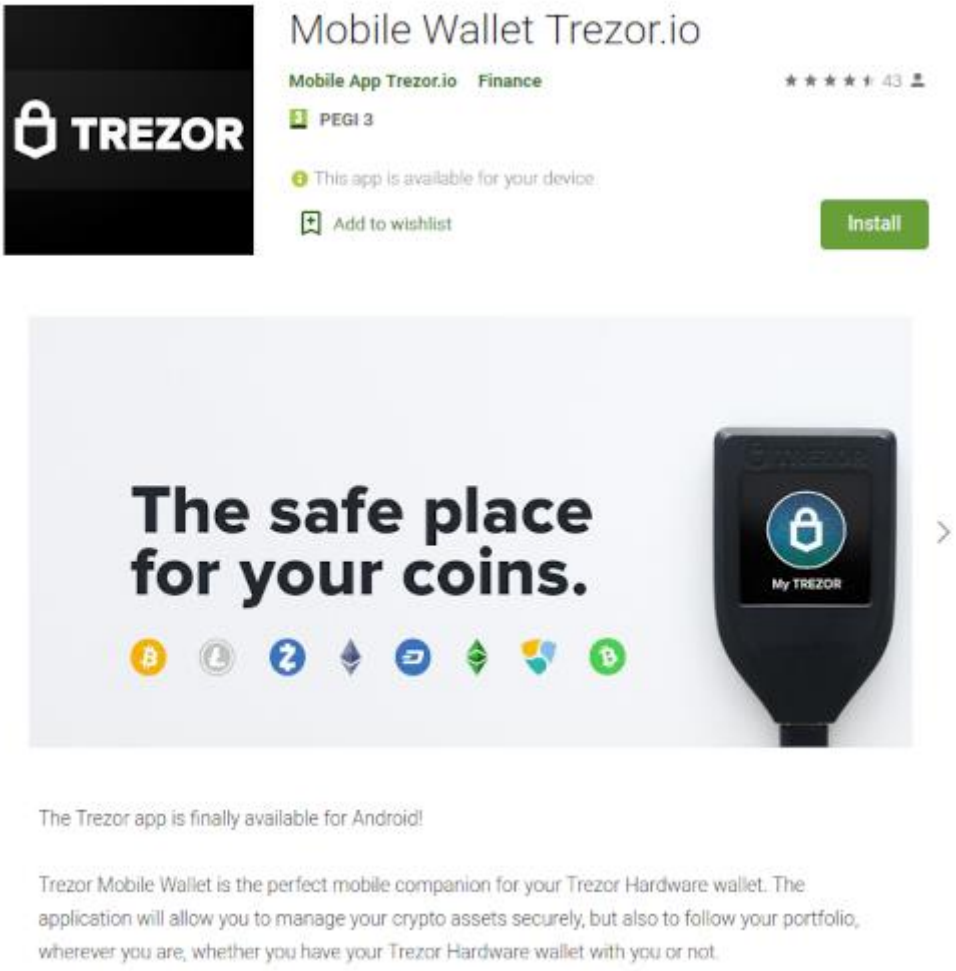
	Ranjivost u pametnom ugovoru	Kao i svaki softver koji se izvodi, tako i pametni ugovori mogu imati ranjivosti uzrokovane greškom programera	Pojedinac	Visoka	Visoka	Visok	Korištenje alata za pronalaženje ranjivosti, npr. *Oyente*

7. Tehnička analiza mobilne aplikacije lažni novčanik

7.1 Mobilne aplikacije „*Trezor Mobile Wallet*“, primjer prvi

U poglavlju 4.3.7. je opisan slučaj u kojem je napadač izradio mobilnu aplikaciju Trezor koristeći zaštitni znak tvrtke *Trezor*, proizvođača hardverskih novčanika. U ovom poglavlju će se napraviti analiza spomenute aplikacija.

Aplikacija se neko vrijeme nalazila u *Play trgovini*, Googleovoj platformi za digitalni sadržaj za Android uređaje, kao legitimna aplikacija (slika 7.1.).

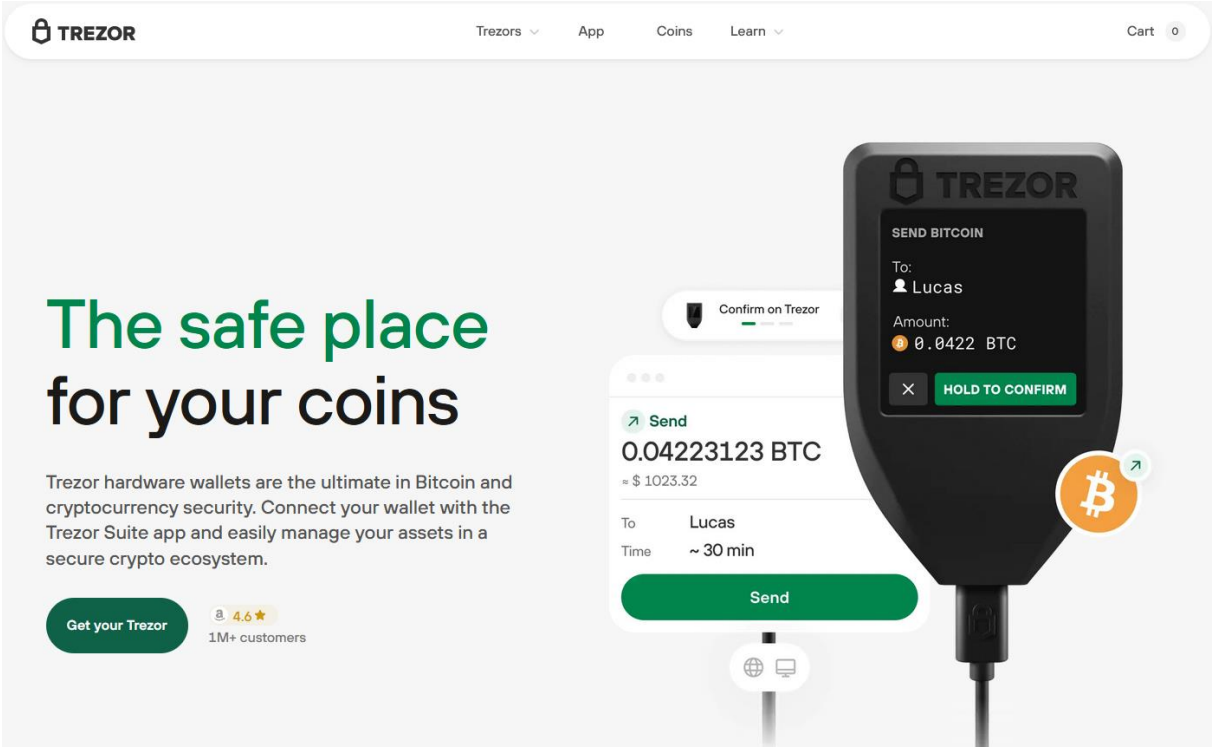


Slika 7.1. *Trezor – zlonamjerni softverski novčanik u Google Play trgovini*

Izvor: Vavkamil.cz [61]

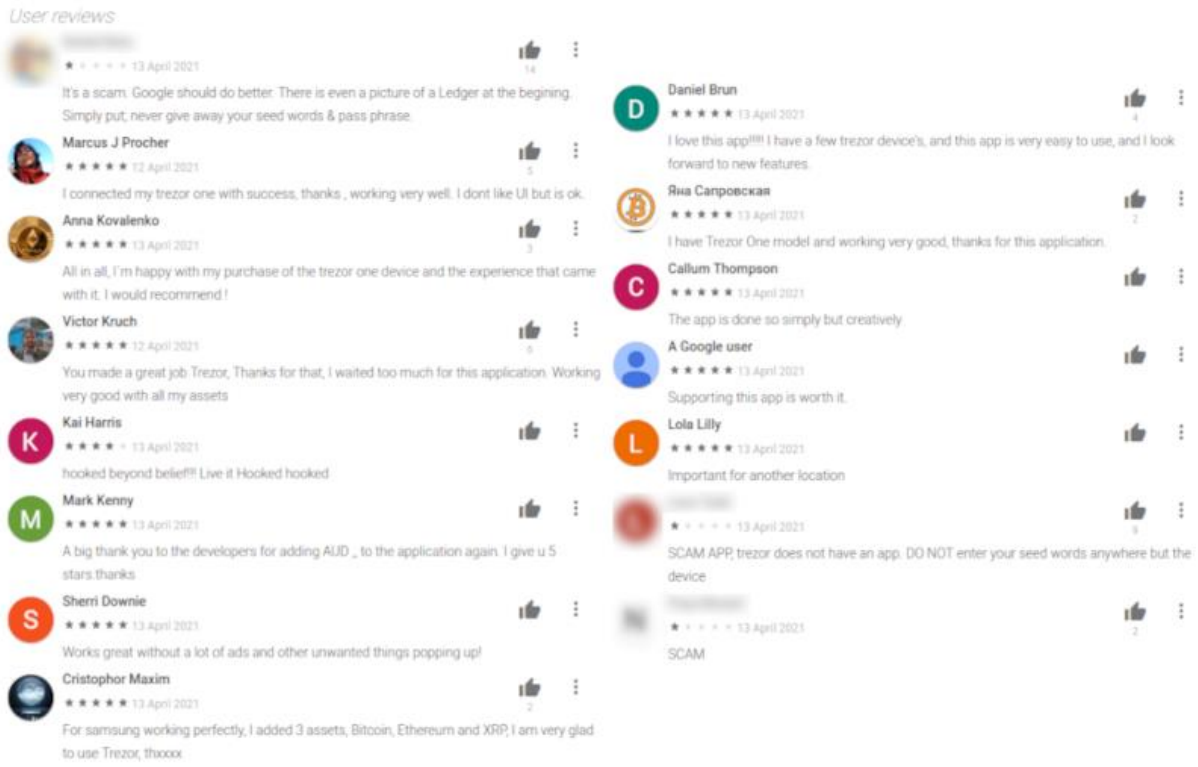
Na slici 7.1. može se vidjeti kako je aplikacija izgledala u *Play trgovini*. Napadač je uspješno koristio zaštitni znak tvrtke *Trezor* te je uspješno lažirao visoku ocjenu od gotovo 5 zvjezdica.

Na slici 7.2. prikazana je legitimna internetska stranica tvrtke *Trezor* i ako napravimo usporedbu možemo vidjeti da je gotovo nemoguće vizualnim pregledom procijeniti da se radi o zlonamjernoj aplikaciji.



Slika 7.2. *Internetska stranica tvrtke „Trezor“*

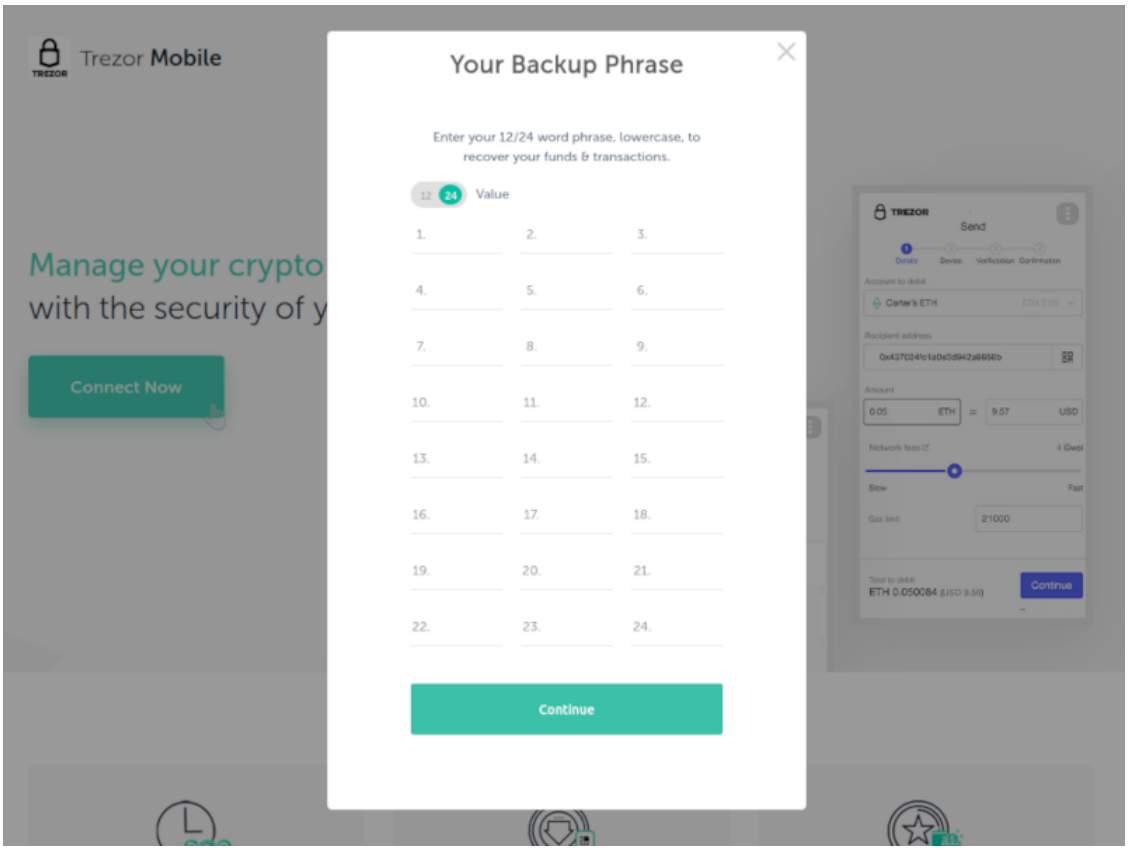
Napadači su se potrudili uvjeriti potencijalne korisnike u vjerodostojnost aplikacije te su napravili nekoliko lažnih recenzija (slika 7.3.). Između većine recenzija, koje su bile ocijenjene s visokih 5 zvjezdica, nalazilo se i nekoliko recenzija koje su pokušale uvjeriti korisnike kako se radi o lažnoj aplikaciji i kako bi trebali izbjegavati skidanje i korištenje aplikacije.



Slika 7.3. *Recenzije mobilne aplikacije Trezor*

Izvor: Vavkamil.cz [61]

Nakon instalacije aplikacije, aplikacija bi prilikom prvog pokretanja zahtijevala da korisnik unese pričuvnu 12/24 frazu (slika 7.4.). Fraza je poznatom svakom korisniku hardverskog novčanika *Trezor*, a za koju bi svaki korisnik hardverskog novčanika trebao znati da ju nigdje nikad ne smije unositi. Na žalost, to u ovom slučaju nije bio slučaj pa su pojedini korisnici unosili, a što su napadači koristili kako bi ukrali sredstva s njihovih računa.



Slika 7.4. *Zahtjev za unos 12/24 fraze riječi prilikom prvog pokretanja lažne aplikacije*

Izvor: Vavkamil.cz [61]

Aplikacija je bila samo web prikaz na zlonamjernu internetsku stranicu i imala je jednu jedinu funkciju, da prikupi fraze riječi korisnika. Kada bi korisnik upisao početnu frazu, Telegramov samostalni računalni program (eng. *bot*) bi poslao šifriranu poruku u grupu, nakon čega bi napadači započeli fazu oporavka kako bi ukrali kriptoimovinu sa korisničkog računa (slika 7.5.).

```php
<?php
    $token = "16308!REDACTED!NyZV60tUX5ptudhtnSLj_nBNdo";

    $data = ["text" => $_POST['seed'],'chat_id' => '-59!REDACTED!38'];

    file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
    return true;
?>
```

Slika 7.5. *Datoteka „seed.php“ je slala zaporke*

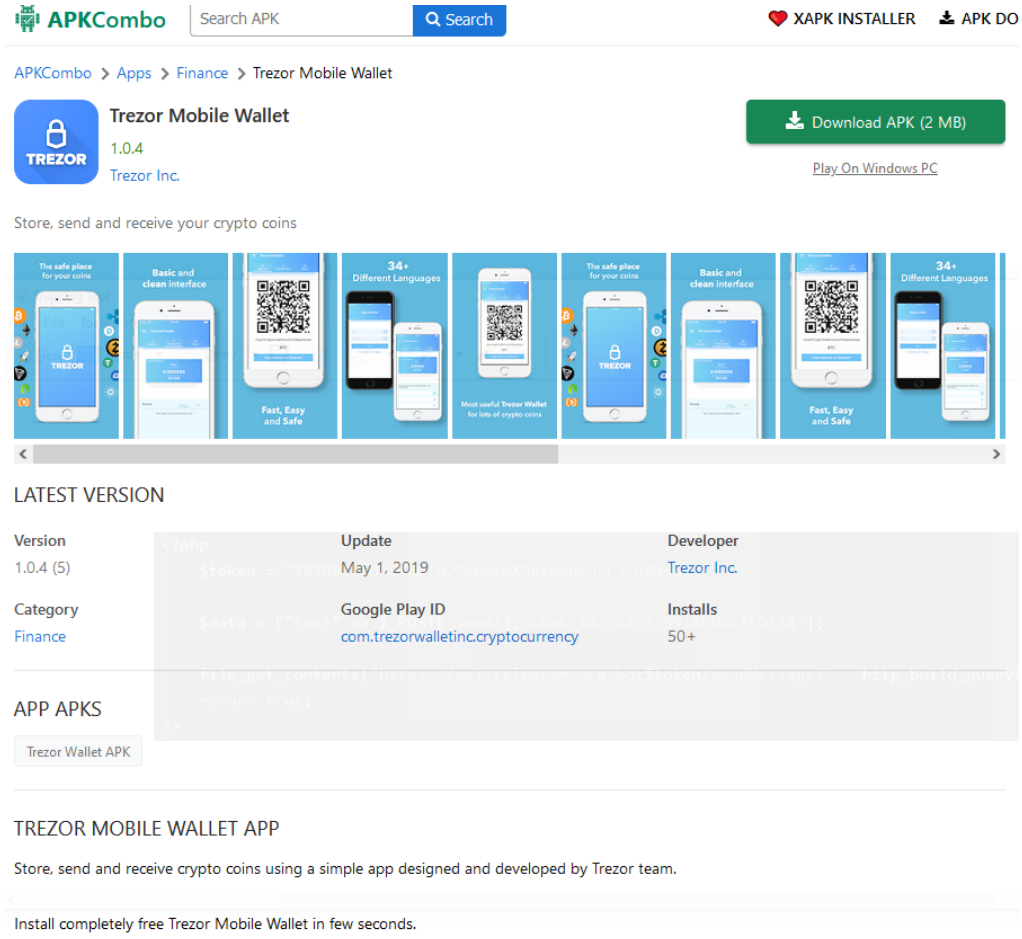
Izvor: Vavkamil.cz [61]

Nakon nekoliko dana, zlonamjerna aplikacija je uklonjena iz trgovine, ali nažalost uspješno je izvršila svoju zadaću. S nekoliko korisničkih računa ukradena je kriptoimovina u vrijednosti od nekoliko milijuna američkih dolara, u tako kratkom vremenskom razdoblju. Na sreću, uklanjanjem ovakvih aplikacija s platformi za distribuciju digitalnog sadržaja, običnom korisniku koji instalira aplikacije samo putem navedenih platformi ona postaje nedostupna. Napredniji korisnici, koji znaju skidati i instalirati aplikacije iz nepoznatih izvora, ovakve aplikacije mogu i dalje naći na internetu i skinuti ih bez da su svjesni štete koju mogu napraviti. U sljedećem slučaju će biti opisan upravo takav slučaj.

7.2 Mobilne aplikacije „*Trezor Mobile Wallet*“, primjer drugi

U trenutku pisanja ovoga rada, s internetske poveznice https://apkcombo.com/trezor-mobile-wallet/com.trezorwalletinc.cryptocurrency se može skinuti aplikacija *Trezor Mobile Wallet*. Iako mobilna aplikacija ima isti naziv kao aplikacija iz prethodnog slučaja, radi se o drugoj aplikaciji, ali s istim ciljem, krađa korisničkih sredstava iz digitalnog novčanika. Radi se o aplikaciji za Android uređaje budući da se na Android uređajima daje mogućnost korisniku da omogući instalaciju aplikacija iz nepoznatih izvora. Zabrana instalacija aplikacija iz nepoznatih izvora je tvornički postavljena na svim Android uređajima, upravo kako bi se onemogućilo korisnicima da instaliraju aplikacije preuzete izvan *Google Play trgovine*, radi njihove zaštite.

Pregledom internetske stranice možemo vidjeti da se koristi Trezorov zaštitni materijal (slika 7.6.)



Slika 7.6. *Zlonamjerna aplikacija Trezor Mobile Wallet je dostupna na internetu*

Na internetskoj stranici možemo vidjeti da je pod razvojnim programerom navedeno „Trezor Inc.“. Kategorija aplikacije, opis aplikacije i slike izgledaju legitimno.

Korištenjem mrežnog alata VirusTotal (https://www.virustotal.com/gui/home/upload) aplikacija je skenirana i 18 proizvođača sigurnosnih rješenja za maliciozne aplikacije je prepoznalo da se radi o malicioznoj aplikaciji (slika 7.7.).

Osnovni podaci o aplikaciji:

MD5 0fdc6eb2667c5e058a766d022976f084

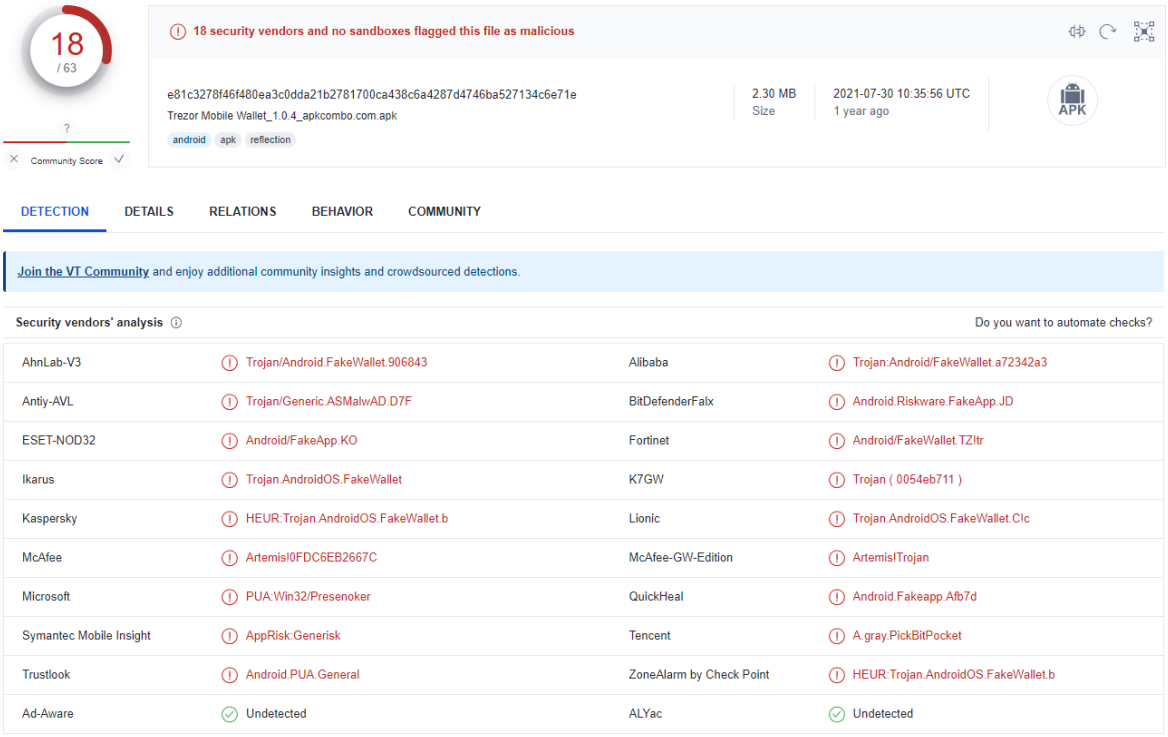
SHA-1 350d976d514d10a4a151c588bcc07975fa6e6f98

SHA-256 e81c3278f46f480ea3c0dda21b2781700ca438c6a4287d4746ba527134c6e71e

Vhash 7526b40e720170ea64eab1e1ba566ce3

SSDEEP
49152:5uM5x5WbS1tcGxh82nsmcOdX0I8C6eeuWDRdi1cPdiASu1m6glwgYt:5uMsOt6hwfe9iHL8mJYt

TLSH	T1FAB50142E349A527C9B7C43387BA077616A64C084A85D75319A6F33C7DBBAC48F85FC8
File type	Android
Magic	Zip archive data, at least v2.0 to extract
TrID	Android Package (57%) Java Archive (20%) Sweet Home 3D design (generic) (15.5%) ZIP compressed archive (5.9%) PrintFox/Pagefox bitmap (640x800) (1.4%)
File size	2.30 MB (2411528 bytes)



Slika 7.7. *Rezultat skeniranja mobilne aplikacije mrežnim alatom VirusTotal*

Zabrinjavajuće je što većina proizvođača sigurnosnih rješenje nije prepoznala aplikaciju kao malicioznu. Neka od njih su renomirani proizvođači. No to nije tema ove analize.

Skeniranjem je utvrđeno da aplikacija ima valjani certifikat koji je izdao Google.

Certificate Attributes

This Android application is signed. When you sign an APK, the signing tool attaches the public-key certificate to the APK. The public-key certificate serves as a fingerprint that uniquely associates the APK to a given developer.

Valid From 2019-05-01 11:21:49

Valid To	2049-05-01 11:21:49
Serial Number	04cc2c462074a251d5b0c3bdf27cb4f7957a24be
Thumbprint	ae241bf8ea4f86bfcfb0403d337eb73ec149133

Certificate Issuer

Distinguished Name	C:US, CN:Android, L:Mountain View, O:Google Inc., ST:California, OU:Android
Common Name	Android
Organization	Google Inc.
Organizational Unit	Android
Country Code	US
State	California
Locality	Mountain View

Dekompiliranjem aplikacije Trezor Mobile Wallet_1.0.4_apkcombo.com.apk utvrđeno je da se u datoteci „\sources\com\wallet\cryptocurrency\ActivityPackage“ nalazi sljedeća linija:

```
final ProgressDialog show =
ProgressDialog.show(LoginActivity.this, "", "", true);
RequestQueue newRequestQueue =
Volley.newRequestQueue(LoginActivity.this);
C04233 r4 = new StringRequest(1,
"https://coinwalletinc.com/nf5/index.php", new
Response.Listener<String>() {
     public void onResponse(String str)
```

Na adresi https://coinwalletinc.com/nf5/index.php se nalazi poslužitelj koji služi za prikupljanje pristupnih podataka korisnika. U vrijeme pisanja ovog rada navedena domena je nedostupna.

Prema opisu aplikacije koji se nalazi na stranici s koje je aplikacija preuzeta, aplikacija omogućava korisnicima stvaranje digitalnog novčanika za razne kriptovalute. Međutim, svrha aplikacije je prevariti korisnike da prebace kriptovalutu u novčanik napadača. Način na koji funkcionira ova prevara je da se aplikacija „pretvara“ da generira jedinstvene adrese novčanika na koju korisnici mogu prenijeti svoju kriptovalutu, a u stvarnosti dodijeljene adrese pripadaju novčaniku napadača jer samo oni imaju privatni ključ potreban za pristup sredstvima. Sve žrtve dobivaju istu adresu novčanika, a napadači imaju jedan novčanik za svaku podržanu kriptovalutu.

Što se tiče grafičkog izgleda, napadači su za kreiranje aplikacije koristili generički predložak za kreiranje kriptonovčanika dostupan za 45 USD na poveznici https://codecanyon.net/item/coinwallet-cryptocurrency-android-wallet-app/21561271 .

8. Zaključak

Iako je tehnologija lanca blokova u primjeni više od 14 godina, danas se o njezinoj široj primjeni, izvan svijeta kriptovaluta, i dalje raspravlja te se traži svrha korištenja tehnologije. Sustavi temeljeni na tehnologiji lanca blokova pokazali su se kao učinkovita metoda za organizaciju velike količine podataka i dobra su alternativa tradicionalnoj bazi podataka. Pored toga, u radu je spomenuto mnogo pothvata i primjera korištenja sustava, iz različitih sektora, temeljenih na tehnologiji lanca blokova, no postavlja se pitanje je li lanac blokova neophodan za bilo koji od njih. Kao glavni argument za primjenu tehnologije lanca blokova se uzima sigurnost, nepromjenjivost zapisa i kopija glavne knjige zapisane na više strana. No nijedan sustav pored nesavjesne i zlonamjerne osobe nije siguran, pa tako ni sustav temeljen na lancu blokova. Sustav povjerenja na kojem se temelji tehnologija lanca blokova je pored takve osobe ugrožen. Procjena rizika tehnologije lanca blokova, uzimajući u razmatranje isključivo ranjivosti same tehnologije bez nenamjernih pogrešaka, pokazala je da se najveća prijetnja u primjeni tehnologije lanca blokova nalazi u ranjivim ili zlonamjernim pametnim ugovorima. Budući da su pametni ugovori jedna od temeljnih prednosti primjene lanca blokova, argument sigurnosti u lancu blokova više nema svoju vrijednost. U radu su opisani slučajevi napada na sustave temeljeni na lancu blokova i moglo se vidjeti da su s vremenom ciljevi napadača postale aplikacije koje čovjek koristi za pristup tim sustavima. Čovjek je uvijek bio i uvijek će ostati najslabija karika svakog lanca te ni jedna tehnologija, bez obzira na stupanj sigurnosti koju pruža, neće moći zaštiti ni jedan sustav od greške samog korisnika. Potrebno je kontinuirano raditi na uvođenju sigurnosnih mjera i provođenju sigurnosnih politika s korisničke točke pristupa sustavu. Na taj će se način zaštiti svaki sustav, bez obzira na tehnologiju koju koristi. Ne treba dizati ruke od tehnologije lanca blokova, ali nije potrebno ni brzati zamjenom postojećih sustava sustavima temeljenim na lancu blokova. Uvođenje svakog novog sustava je skupo, a pitanje je pruža li taj sustav ono što očekujemo od njega. Od tehnologije lanca blokova se ima velika očekivanja, ali zaključak je da njena implementacija ne donosi velike prednosti s velikim troškovima koje implementacija zahtijeva. Razvijene sigurnosne mjere i provođenje sigurnosne politike nad tradicionalnim sustavima pružaju dovoljnu sigurnost tih sustava.

9. Literatura

[1] S. Haber i W. S. Stornetta, »SpringerLink,« [Mrežno]. Available: https://link.springer.com/content/pdf/10.1007/BF00196791.pdf?pdf=inline%20link. [Pristup 16. prosinca 2022.].

[2] A. Gupta, »Introduction to Blockchain technology,« GeeksforGeeks, 22. prosinca 2022. [Mrežno]. Available: https://www.geeksforgeeks.org/blockchain-technology-introduction/?ref=leftbar-rightbar. [Pristup 22. prosinac 2022.].

[3] T. Bareman, »EU regulator calls for a ban on proof of work Bitcoin mining to save renewable energy,« Euronews, 20. siječnja 2022.. [Mrežno]. Available: https://www.euronews.com/next/2022/01/19/eu-regulator-calls-for-a-ban-on-proof-of-work-bitcoin-mining-to-save-renewable-energy. [Pristup 25. prosinac 2022.].

[4] IBM, »What are smart contacts on blockchain?,« IBM, [Mrežno]. Available: https://www.ibm.com/topics/smart-contracts. [Pristup 28. prosinac 2022.].

[5] A. Y. Y. A. F. Abas, »Expanding the Data Capacity of QR Codes Using Multiple Compression Algorithms and Base64 Encode/Decode,« 1. lipnja 2017. [Mrežno]. Available: https://jtec.utem.edu.my/jtec/article/view/2217. [Pristup 29. prosinca 2022.].

[6] R. Merkle, »Protocols for public key cryptosystems,« *Proceedings of the 1980 IEEE Symposium on Security and Privacy, IEEE, Oakland, CA, USA,* pp. 122-134, 1980.

[7] K. Collier, »North Korea stole a record $400 million in cryptocurrency last year, researchers say,« NBC News, 13. siječnja 2022. [Mrežno]. Available: https://www.nbcnews.com/tech/security/north-korea-stole-record-400-million-cryptocurrency-last-year-research-rcna12080. [Pristup 30. prosinca 2022.].

[8] Digital Assets d.o.o., »Bitcoin store,« Digital Assets d.o.o., 1. veljače 2022. [Mrežno]. Available: https://www.bitcoin-store.hr/blog/sto-je-pametni-ugovor/. [Pristup 2. siječnja 2023.].

[9] N. Szabo, »The many traditions of non-governmental money (part i),« 1997. [Mrežno]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html. [Pristup 20. siječnja 2023.].

[10] Your Europe, »Zaštita podataka na temelju Opće uredbe o zaštiti podataka,« Your Europe, 6. lipnja 2022. [Mrežno]. Available: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm. [Pristup 2. siječnja 2023.].

[11] J. L. Brad Polizzano, »The Tax Adviser,« AICPA & CIMA, 1. listopada 2018. [Mrežno]. Available: https://www.thetaxadviser.com/issues/2018/oct/cryptocurrency-compliance-challenges-irs-enforcement.html. [Pristup 3. siječnja 2023.].

[12] Wikipedia, »Coinbase,« Wikipedia, 29. prosinca 2022. [Mrežno]. Available: https://en.wikipedia.org/wiki/Coinbase. [Pristup 3. siječnja 2023.].

[13] N. Kshetri, »Blockchain's roles in strengthening cybersecurity and protecting privacy,« 2017. [Mrežno]. Available: http://libres.uncg.edu/ir/uncg/f/N_Kshetri_Blockchain_2017.pdf. [Pristup 3. siječnja 2023.].

[14] Coinmarketcap, »Today's Cryptocurrency Prices by Market Vap,« Coinmarketcap, 3. siječnja 2023. [Mrežno]. Available: https://coinmarketcap.com/. [Pristup 3. siječnja 2023].

[15] F. Hersey, »South Korea's digital identity blockchain prepares to add new credentials, go international,« Biometric update.com, 27. prosinca 2022. [Mrežno]. Available: https://www.biometricupdate.com/202212/south-koreas-digital-identity-blockchain-prepares-to-add-new-credentials-go-international. [Pristup 4. siječnja 2023.].

[16] A. Macdonald, »Researchers advocates make case for more inclusive digital id systems in id4africa livecast,« Biometric update.com, 22. studenog 2021. [Mrežno]. Available: https://www.biometricupdate.com/202111/researchers-advocates-make-case-for-more-inclusive-digital-id-systems-in-id4africa-livecast. [Pristup 6. siječnja 2023.].

[17] G. Greenspan, »Avoiding the pointless blockchain project,« MultiChain, 22. studenog 2015. [Mrežno]. Available: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/. [Pristup 6. siječnja 2023.].

[18] A. Singh, S. MacConnell, N. Hong, M. Aranke i C. Noble, »A Model for Genetic Data Exchange and Sovereignty,« 2018. [Mrežno]. Available: https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5e583c097e83fd0007cf2bb6/1582840842756/A+Model+for+Genetic+Data+Exchange+and+Sovereignty-2.pdf. [Pristup 6. siječnja 2023.].

[19] PWC, »Threats to the Financial Services sector,« 2014. [Mrežno]. Available: https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf. [Pristup 7. siječnja 2023.].

[20] Wikipedia, »Zero-knowledge proof,« Wikipedia, 15. prosinca 2022. [Mrežno]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof. [Pristup 7. siječnja 2023.].

[21] Oliver Wyman, Anthemis Group and Santander Innoventures, »The Fintech 2.0 Paper: rebooting financial services,« 2015. [Mrežno]. Available: https://www.finextra.com/finextra-

downloads/newsdocs/the%20fintech%202%200%20paper.pdf. [Pristup 7. siječnja 2023.].

[22] Euromoney learning, »The rise of private blockchains,« Euromoney learning, [Mrežno]. Available: https://www.euromoney.com/learning/blockchain-explained/the-rise-of-private-blockchains. [Pristup 20. siječnja 2023.].

[23] R. Recabarren i B. Carbunar, »Hardening Stratum, the Bitcoin Pool Mining Protocol,« [Mrežno]. Available: https://users.cs.fiu.edu/~carbunar/bedrock.pdf. [Pristup 20. siječnja 2023.].

[24] A. Z. a. L. V. Maria Apostolaki, »Hijacking Bitcoin: Routing Attacks on Cryptocurrencies,« u *IEEE Symposium on Security and Privacy*, 2017.

[25] O. Avan-Nomayo, »Bitcoin network node count sets new all-time high,« 15. lipnja 2021. [Mrežno]. Available: https://cointelegraph.com/news/bitcoin-network-node-count-sets-new-all-time-high. [Pristup 20. siječnja 2023.].

[26] K. Groves, »Cryptocurrency Exchange Hacks (Updated List For 2023),« HedgewithCrypto, 17. siječnja 2023. [Mrežno]. Available: https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/. [Pristup 22. siječnja 2023.].

[27] D. Pollock, »The Mess That Was Mt. Gox: Four Years On,« Cointelegraph, 9. ožujka 2018. [Mrežno]. Available: https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on. [Pristup 3. veljače 2023.].

[28] R. McMillan, »Bitcoin Exchange Mt. Gox Goes Offline Amid Allegations of $350 Million Hack,« Wired, 24. veljače 2014.. [Mrežno]. Available: https://www.wired.com/2014/02/bitcoins-mt-gox-implodes-2/. [Pristup 3. veljače 2023.].

[29] Internet archive, »Mt. Gox Situation Crisis Strategy Draft,« Internet archive, 224. veljače 2014. [Mrežno]. Available: https://archive.org/details/MtGoxSituationCrisisStrategyDraft/page/n3/mode/2up. [Pristup 22. veljače 2023.].

[30] MtGox, »MtGox,« 20. ožujka 2014. [Mrežno]. Available: https://www.mtgox.com/img/pdf/20140320-btc-announce.pdf. [Pristup 3 veljače 2023.].

[31] Blockchain.com, »Binance Hack,« Blockchain, 7. svibnja 2019. [Mrežno]. Available: https://www.blockchain.com/explorer/transactions/btc/e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea. [Pristup 3 veljače 2023.].

[32] G. Weston, »Importance Of TVL (Total Value Locked) In DeFi,« 101 Blockchains, 11. lipnja 2022. [Mrežno]. Available: https://101blockchains.com/total-value-locked-in-defi/. [Pristup 3. veljače 2023.].

[33] Tiana, »10 most common forms of DeFi attacks and how to prevent them,« Coin98 insights, 31. srpnja 2022. [Mrežno]. Available: https://coin98.net/10-most-common-forms-of-defi-attacks. [Pristup 7. veljače 2023.].

[34] Uniswap.org, »Uniswap V2 Overview,« Uniswap, 23. ožujka 2020. [Mrežno]. Available: https://uniswap.org/blog/uniswap-v2. [Pristup 7. veljače 2023.].

[35] Bitcoin store, »Što je stablecoin i kako funkcionira? Vodič za početnike,« Bitcoin store, 25. ožujka 2022. [Mrežno]. Available: https://www.bitcoin-store.hr/blog/sto-je-stablecoin-i-kako-funkcionira/. [Pristup 7. veljače 2023.].

[36] C. Faife, »Beanstalk cryptocurrency project robbed after hacker votes to send themself $182 million,« The Verge, 18. travnja 2022. [Mrežno]. Available: https://www.theverge.com/2022/4/18/23030754/beanstalk-cryptocurrency-hack-182-million-dao-voting. [Pristup 8. veljače 2023.].

[37] Certik, »Revisiting Beanstalk Farms Exploit,« Certik, 28. lipnja 2022. [Mrežno]. Available: https://www.certik.com/resources/blog/6HaLMGIL5sI2fpfEZc0nzS-revisiting-beanstalk-farms-exploit. [Pristup 8. veljače 2023.].

[38] Ethereum.org, »WEB2 VS WEB3,« Ethereum, 26. rujna 2022. [Mrežno]. Available: https://ethereum.org/en/developers/docs/web2-vs-web3/. [Pristup 8. veljače 2023.].

[39] MetaMask Support, »Basic Safety and Security Tips for MetaMask,« MetaMask, 2022. [Mrežno]. Available: https://metamask.zendesk.com/hc/en-us/articles/360015489591-Basic-Safety-and-Security-Tips-for-MetaMask. [Pristup 8. veljače 2023.].

[40] D. Finlay, »Phisher Watch: Airdrop Scams,« Medium, 26. prosinca 2021. [Mrežno]. Available: https://medium.com/metamask/phisher-watch-airdrop-scams-82eea95d9b2a. [Pristup 8. veljače 2023.].

[41] Harry, »Hunting Huobi, MyEtherWallet, and Blockchain.info Scams,« Medium, 14. svibnja 2019. [Mrežno]. Available: https://medium.com/mycrypto/hunting-huobi-scams-662256d76720. [Pristup 8. veljače 2023.].

[42] J. B. Merrill, »Read that link carefully: Scammers scoop up misspelled cryptocurrency URLs to rob your wallet,« The Washington Post, 8. listopada 2021. [Mrežno]. Available: https://www.washingtonpost.com/technology/2021/10/08/cryptocurrency-scam-websites/. [Pristup 8. veljače 2023.].

[43] R. Behnke, »Ice phishing threat to the ERC-20 tokens on the Blockchain,« Halborn, 6. ožujka 2022. [Mrežno]. Available: https://halborn.com/ice-phishing-threat-to-the-erc-20-tokens-on-the-blockchain/. [Pristup 9. veljače 2023.].

[44] Rekt, »Badger - REKT,« Rekt, 2. prosinca 2021. [Mrežno]. Available: https://rekt.news/badger-rekt/. [Pristup 9. veljače 2023.].

[45] M. Shen, »Crypto Lender Celsius Admits Losses in $120M BadgerDAO Hack,« Coindesk, 3. prosinca 2021. [Mrežno]. Available:

https://www.coindesk.com/markets/2021/12/03/crypto-lender-celsius-admits-losses-in-120m-badgerdao-hack/. [Pristup 9. veljače 2023.].

[46] Kaspersky, »Over half of ransomware victims pay the ransom, but only a quarter see their full data returned,« Kaspersky, 30. ožujka 2021. [Mrežno]. Available: https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned. [Pristup 10. veljače 2023.].

[47] O. Delgado-Mohatar, J. M. Sierra-Camara i E. Anguiano, »Blockchain-based semi-autonomous ransomware,« 13. lipnja 2020. [Mrežno]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X19317406. [Pristup 11. veljače 2023.].

[48] C. Cimpanu, »Two SIM swappers arrested for CMCT hack,« ZDnet, 30. rujna 2018.. [Mrežno]. Available: https://www.zdnet.com/article/two-sim-swappers-arrested-for-cmct-hack/. [Pristup 11. veljače 2023.].

[49] D. Palmer, »Victims Sue AT&T, T-Mobile Over 'SIM Swap' Crypto Hacks,« Coindesk, 9. studenog 2018. [Mrežno]. Available: https://www.coindesk.com/markets/2018/11/09/victims-sue-att-t-mobile-over-sim-swap-crypto-hacks/. [Pristup 13. veljače 2023.].

[50] Tezro, »Hardware Wallet vs. Software Wallet: What is the Difference?,« Tezro, 8 veljače 2023. [Mrežno]. Available: https://blog.tezro.com/hardware-wallet-vs-software-wallet/. [Pristup 14. veljače 2023.].

[51] Statista, »Number of available applications in the Google Play Store from December 2009 to September 2022,« Statista, 14. studenog 2022. [Mrežno]. Available: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/. [Pristup 14. veljače 2023.].

[52] Statista, »Number of available apps in the Apple App Store from 1st quarter 2015 to 3rd quarter 2022,« Statista, 8. studenog 2022. [Mrežno]. Available: https://www.statista.com/statistics/779768/number-of-available-apps-in-the-apple-app-store-quarter/. [Pristup 14. veljače 2023.].

[53] J. Grand, »Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries),« Youtube, 14. Maožujka 2011. [Mrežno]. Available: https://www.youtube.com/watch?v=VVJldn_MmMY. [Pristup 14. veljače 2023.].

[54] K. Zetter, »Cracking a $2 million crypto wallet,« The Verge, 24. siječnja 2022. [Mrežno]. Available: https://www.theverge.com/2022/1/24/22898712/crypto-hardware-wallet-hacking-lost-bitcoin-ethereum-nft. [Pristup 14. veljače 2023.].

[55] R. Albergotti, »He believed Apple’s App Store was safe. Then a fake app stole his life savings in bitcoin.,« The Seattle Times, 4. travnja 2021. [Mrežno]. Available:

https://www.seattletimes.com/business/technology/he-believed-apples-app-store-was-safe-then-a-fake-app-stole-his-life-savings-in-bitcoin/. [Pristup 15. veljače 2023.].

[56] Service NSW, »Licence checkers and the NSW Digital Driver Licence,« NSW Goverment, 8 veljače 2023. [Mrežno]. Available: https://www.service.nsw.gov.au/campaign/nsw-digital-driver-licence/licence-checkers-and-the-nsw-digital-driver-licence. [Pristup 19. veljače 2023.].

[57] D. Goodin, »'Tough to Forge' Digital Driver's Licenses Are—Yep—Easy to Forge,« Ars Technica, 5. svibnja 2022.. [Mrežno]. Available: https://arstechnica.com/information-technology/2022/05/digital-drivers-license-used-by-4m-australians-is-a-snap-to-forge/. [Pristup 19. veljače 2023.].

[58] 101 Blockchains, »Blockchain Risk Assessment and Enterprise Management Framework,« 101 Blockchains, 29. rujna 2021. [Mrežno]. Available: https://101blockchains.com/enterprise-blockchain-risk-assesment/. [Pristup 22. veljače 2023.].

[59] J. T. F. T. Initiative, »SP 800-30 Rev. 1, Guide for Conducting Risk Assessments,« 17. rujna 2012.. [Mrežno]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. [Pristup 27. travnja 2023.].

[60] Timothy Casey, Intel Corporation, »Threat Agent Library Helps Identify Information Security Risks,« rujan 2007. [Mrežno]. Available: https://www.oasis-open.org/committees/download.php/66239/Intel%20Corp_Threat%20Agent%20Library_07-2202w.pdf. [Pristup 27. travnja 2023.].

[61] K. Vavra, »Analysis of the Fake Trezor Mobile Wallet app in the Play Store,« 14. travnja 2021.. [Mrežno]. Available: https://vavkamil.cz/2021/04/14/analysis-of-the-fake-trezor-mobile-wallet-app-in-the-play-store/. [Pristup 24. veljače 2023.].

Životopis

Edin Gosić je završio diplomski studij Informatike na Odjelu za informatiku Sveučilišta u Rijeci. Karijeru je započeo u 2005. godine nakon završenog stručnog studija Elektrotehnike na Tehničkom fakultetu u Rijeci na poslovima mrežnog inženjera. Tijekom godina stjecao je mnoge profesionalne certifikate iz područja mrežne tehnologije, usko se specijalizirajući za sigurnosna mrežna rješenja. Danas radi kao projektni inženjer u Zenitel Mediterranean d.o.o. projektirajući mrežne sustave za plovila u pomorstvu.

Edin Gosic graduated in computer science from the Department of Computer Science, University of Rijeka. He started his career in 2005 after completing the program Electrical Engineering at the Technical Faculty in Rijeka as a network engineer. Over the years, he has acquired numerous professional certifications in network technology, specializing in network security solutions. Today he works as a project engineer at Zenitel Mediterranean d.o.o. designing a network solution system for the maritime industry.