Sigurnost ulančanih blokova

Šimundić, Marin

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

SIGURNOST ULANČANIH BLOKOVA

Završni rad

Marin Šimundić

Osijek, 2023.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 26.06.2023.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Marin Šimundić
Studij, smjer:	Računalno inženjerstvo
Mat. br. Pristupnika, godina	R4571, 27.07.2020.
OIB Pristupnika:	92593988789
Mentor:	izv. prof. dr. sc. Ivica Lukić
Sumentor:	Miljenko Švarcmajer, mag. ing. comp.
Sumentor iz tvrtke:	
Naslov završnog rada:	Sigurnost ulančanih blokova
Znanstvena grana rada:	**Informacijski sustavi (zn. polje računarstvo)**
Zadatak završnog rad:	Dati pregled područja lanca ulančanih blokova (engl. Blockchain) te kako njegova sigurnost utječe na kompletan sustav lanca ulančanih blokova. Navesti najčešće sigurnosne rizike i predložiti mjere kako bi se spriječili napadi na mrežu. Tema je rezervirana za: Marin Šimundić
Prijedlog ocjene završnog rada:	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene od strane mentora:	26.06.2023.
Datum potvrde ocjene od strane Odbora:	12.07.2023.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

IZJAVA O ORIGINALNOSTI RADA

Osijek, 12.07.2023.

Ime i prezime studenta:	Marin Šimundić
Studij:	Računalno inženjerstvo
Mat. br. studenta, godina upisa:	R4571, 27.07.2020.
Turnitin podudaranje [%]:	5

Ovom izjavom izjavljujem da je rad pod nazivom**: Sigurnost ulančanih blokova**

izrađen pod vodstvom mentora izv. prof. dr. sc. Ivica Lukić

i sumentora Miljenko Švarcmajer, mag. ing. comp.

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

Potpis studenta:

SADRŽAJ

1. UVOD

Lanac blokova (engl. *blockchain*) je inovativna tehnologija koja je u posljednjem desetljeću privukla veliku pažnju različitih industrija i sektora. Ova tehnologija omogućuje decentraliziranu pohranu i prijenos podataka te se smatra revolucionarnim konceptom koji može transformirati način na koji se odvija razmjena vrijednosti, vjerodostojnost podataka i sigurnost transakcija. Porastom popularnosti upotrebe lanca blokova dovodi se u pitanje sigurnost korištenja istih.

Ovaj završni rad ima za cilj pružiti pregled područja lanca blokova i istražiti kako sigurnost ove tehnologije utječe na cjelokupni sustav. Uz to, rad će se usredotočiti na identificiranje najčešćih sigurnosnih rizika koji se mogu pojaviti u lancu blokova te će predložiti različite mjere koje se mogu poduzeti kako bi se spriječili napadi na mrežu.

1.1. Zadatak završnog rada

Ovaj rad ima zadatak provesti čitatelja kroz svijet lanca blokova, način na koji on radi, načine korištenja te upoznati čitatelja sa sigurnosnim rizicima i napadima. Čitatelj se, na početku, upoznaje s terminologijom kroz teorijsku podlogu u kojoj ćemo dati definiciju lanca blokova, opisati strukturu, upoznati se s vrstama i karakteristikama blokova te, naposljetku, objasniti pojam kriptografije i enkripcije u lancu blokova. Upoznavanje sa sigurnosnim rizicima i napadima na lanac blokova od velike je važnosti pošto je tema rada "Sigurnost ulančanih blokova". Istražit ćemo nekoliko vrsta napada i ranjivosti cjelokupnog sustava te dati pregled najvećih napada do sada uz primjere rješenja za sprječavanje takvih napada. Nadalje, istražit će se tehničke, organizacijske i pravne mjere za jačanje sigurnosti lanca blokova. Naposljetku, pružit će se primjeri korištenja lanca blokova u svakodnevnom životu te dati primjeri sektora koji koriste ovu tehnologiju.

2. PREGLED PODRUČJA RADA

Tehnologija lanca blokova dostigla je veliku popularnost u zadnjem desetljeću zbog zamisli i tehnologiji na kojoj se temelji. Glavna zamisao tehnologije lanca blokova je stvoriti decentralizirani sustav u kojem svatko vodi vlastite evidencije transakcija. Tehnologija lanca blokova doživjela je popularnost u različitim sektorima zbog svojih karakteristika i potencijala, najviše u svijetu kriptovaluta. Detaljniji podaci o pojmu kriptovaluta mogu se pregledati na [1]. Ideja tehnologije lanca blokova jest stvoriti decentralizirani sustav koji se ne može lako pratiti i nadgledati. Potreba za tehnologijom lanca blokova javila se zbog ubrzanja transakcija te izbjegavanja treće strane (engl. *third party*). Treća strana je entitet koji sudjeluje u interakciji između dva druga entiteta. Također, postoje tri vrste blokova unutar lanca o kojima će više biti rečeno u narednim odjeljcima. U pitanje dolazi sigurnost cijelog sustava jer se tehnologija zasniva na transakcijskoj prirodi. Neki od najzastupljenijih vrsta napada su *napad 51%*, *Problem dvostruke potrošnje*, *Sybil*, *Krađa identiteta* te *ranjivosti pametnim ugovorima* o kojem će biti rečeno nešto više u razradi ovog rada.

Ovaj rad pokriva područje općenite upotrebe tehnologije lanca blokova te razmatra sigurnosne rizike i napade na sustav. Područje upotrebe tehnologije lanca blokova je vrlo opširno te će se ovaj rad baviti općenitim upotrebama u svakodnevnom životu.

Kao što je prije rečeno, u sljedećim poglavljima opisivati će se tehnologija lanca blokova, razmatrati sigurnosni rizici i napadi te uvidjeti mjere sigurnosti i razmatrati sektori u kojima je najzastupljenija tehnologija lanca blokova.

3. TEORIJSKA PODLOGA

U narednom poglavlju opisat će se teorijska podloga lanca blokova, dati definicija i djelovanje, opisati glavne dijelove te imenovati i opisati glavne vrste i karakteristike blokova. Također, objasnit će se pojam kriptografije i enkripcije u lancu blokova.

3.1. Definicija lanca blokova i njegovog djelovanja

Lanac blokova, prema [2], predstavlja podijeljenu strukturu podataka, odnosno listu informacija podijeljenih između svih čvorova u sustavu. Tehnologija lanca blokova prvi put se pojavila 1991. godine te je dobila pažnju nastankom Decentralizirane Autonomne Organizacije (DAO). To je novi oblik pravne strukture koja nema središnje upravljačko tijelo i čiji članovi dijele zajednički cilj djelovanja u najboljem interesu subjekta [3] . Prvi praktični primjer DAO-a uveden je 2009. godine u obliku kriptovalute Bitcoin. Po prvi put, Satoshi Nakamoto objavio je kratki rad pod naslovom *Bitcoin: Peer-to-Peer elektronički gotovinski sustav*, koji je pokrio koncept i rad sustava kriptovaluta kao DAO [4].

Razlikujemo tri glavna tipa arhitekture lanca blokova: javni, privatni, konzorcijski ili federalni [5]. Također, postoji i četvrti, hibridni tip, koji je kombinacija javnog i privatnog tipa.

Javni blok je otvoren javnosti i unutar njega svatko može sudjelovati kao čvor u donošenju odluka. Svaki čvor, odnosno korisnik, ima kopiju javne knjige (engl. *ledger*) te koristi distribuirani mehanizam konsenzusa zbog donošenja odluka o daljnjem stanju lanca blokova.

Privatni blok je privatan i otvoren samo određenoj grupi korisnika. U ovakvom sustavu osoba, korporacija ili institucija u potpunosti kontrolira sve čvorove unutar Peer-to-Peer mreže. Drugim riječima, samo administrator lanca može odobriti ulazak korisnicima u mrežu.

Konzorcijski ili federalni blok je sličan privatnom no za razliku od njega ima više administratora, to jest, glavnih korisnika u mreži. Za ulazak u konzorcijski blok, korisnik može biti zatražen platiti početnu pristojbu (engl. *fee*).

3.2. Komponente lanca blokova

Glavni proces u lancu blokova je dodavanje zapisa o transakcijama u javnu knjigu koja sadrži popis svih prijašnjih transakcija. Zbirka zapisa naziva se blok, a javna knjiga svih prijašnjih transakcija se naziva lanac blokova.

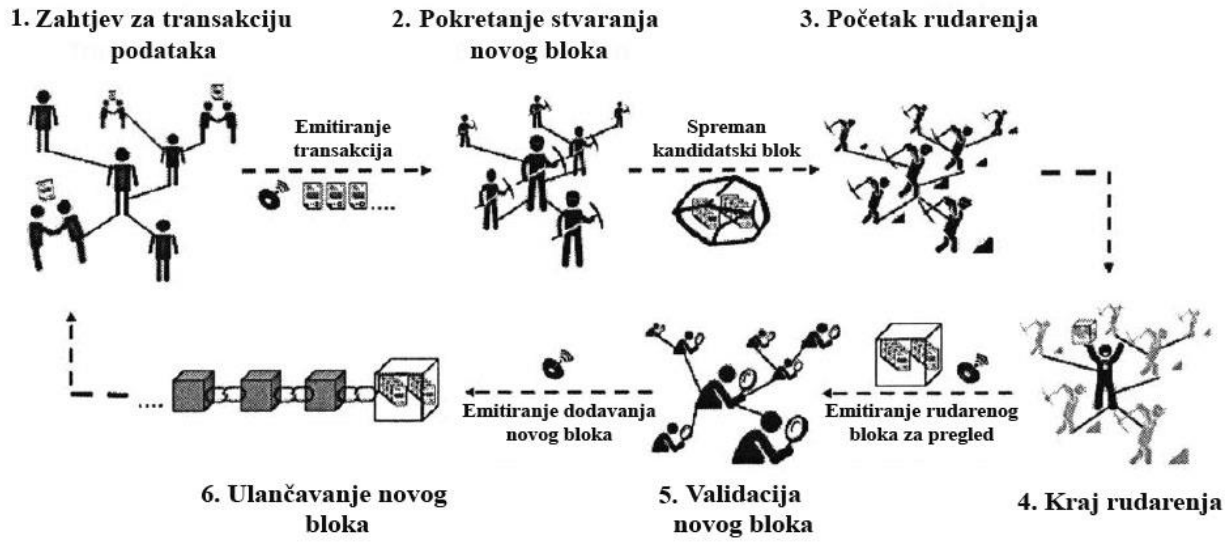
Podatkovna struktura i procesi u lancu blokova ovise o konsenzus mehanizmu koji se koristi. Postoje različiti konsenzusi u lancima blokova, kao što su Proof of Work (PoW), Proof of Stake

(PoS), Delegated Proof of Stake (DPoS) i drugi. Svaki od tih konsenzusa ima svoje karakteristike i načine rješavanja problema.

U tehnologiji lanca blokova, bez obzira na korišteni konsenzus, blokovi su povezani putem adresne vrijednosti (engl. *hash*). Svaki blok sastoji se od podatka, svojeg hash-a i hash-a prethodnog bloka u lancu. Hash predstavlja jednosmjernu matematičku funkciju koja daje tekst sažetka nekog teksta koristeći odgovarajući algoritam sažimanja. Bez obzira na konsenzus, hash je uvijek iste duljine, neovisno o duljini podatka prije kriptiranja.

U Proof of Work konsenzusu, rudari (engl. *miners*) se natječu u rješavanju matematičkih problema temeljenih na kriptografskom *hash* algoritmu [6]. Rudarenjem potvrđuju nove transakcije i dodaju ih u lanac blokova. Međutim, proces potvrđivanja transakcija u drugim konsenzusima izgleda drugačije.

Lanac blokova odgovoran je za ovjeravanje dolaska transakcije u mrežu. Čvor, odnosno korisnik mreže, provjerava valjanost transakcije i sprječava pokušaje zlouporabe ili izmjene legitimnih podatkovnih transakcija. Na taj način niti jedan pojedinačni čvor unutar mreže ne može promijeniti informacije koje se unutar njega nalaze. Zbog svoje popularnosti i zastupljenosti, proces unutar lanca blokova prikazat ćemo na primjeru PoW konsenzusa. Proces je, prema slici 3.1., podijeljen u šest faza: zahtjev za transakciju podataka, pokretanje stvaranja novog bloka, početak rudarenja, kraj rudarenja, validacija novog bloka i ulančavanje novog bloka.



Slika 3.1. *Pregled dodavanja bloka u lanac blokova*

1. Zahtjev za transakciju podataka

Čvorovi su korisnici koji imaju pristup mreži (obično putem interneta) lanca blokova, koja pohranjuje sve transakcijske podatke od samog početka u obliku lanca informacija koji se nazivaju blokovi [7]. Emitiranje podataka cijeloj mreži sustava započinje nakon što bilo koja dva čvora započnu podatkovnu transakciju. Primjer toga vidimo u sustavu kriptovaluta gdje je podatkovna transakcija informacija o kretanju kriptovalute od jednog čvora do drugog. U tom procesu bilježi se adresa pošiljatelja, primatelja, vrijeme pokretanja i količina kriptovalute.

2. Pokretanje stvaranja novog bloka

Svaki rudar je odgovoran za provjeru valjanosti novih podatkovnih transakcija i njihovo evidentiranje u javnoj knjizi. U ovoj početnoj fazi prije stvarnog rudarenja, svaki rudar neovisno provjerava valjanost svih novih dolaznih transakcijskih podataka, kao što je usklađenost s protokolom lanca, provjera identiteta pomoću digitalnih potpisa i sukobi s prethodno pregledanim transakcijama [8]. Nakon što se potvrdi valjanost podataka, rudar počinje organizirati transakcije kao dio kandidatskih blokova koje rudar izrađuje pojedinačno i lokalno no u ovoj fazi blokovi nisu još dio lanca. Rudari nastavljaju grupirati sve valjane transakcije u kandidatske blokove sve dok blok kandidat ne dosegne unaprijed definirano ograničenje veličine postavljeno protokolom. Kada je kandidatski blok spreman za rudarenje, rudar bilježi vremensku oznaku informacijske transakcije i *hash* vrijednost prethodnog bloka u zaglavlje kandidatskog bloka. Uz pomoć vremenskih oznaka, lanac blokova može linearno ulančati podatke kako bi se izbjeglo dupliciranje.

3. Početak rudarenja

Nakon dovršetka kandidatskog bloka, rudar započinje proces rudarenja koji se temelji na rješavanju zagonetki za dobivanje kriptografske vrijednosti, odnosno *Proof-of-Work* (PoW). Rudarenje se izvodi koristeći *hash* funkciju koja služi kao algoritam rješavanja zagonetke kandidatskog bloka.

4. Kraj rudarenja

Nakon što je zagonetka uspješno riješena, rudar može dovršiti proces rudarenja dodavanjem *hash* vrijednosti u zaglavlje bloka. Blokovi, unutar svojeg zaglavlja, moraju sadržavati vlastiti PoW da bi se smatrali valjanim. Mala vjerojatnost i nepredvidljivost PoW-a stoga služi kao

važna zaštita za sustav Blockchain za rješavanje pitanja sigurnosti i integriteta podataka bez središnje kontrole [9].

5. Validacija novog bloka

Sljedeći koraci su prosljeđivanje bloka, emitiranje na mrežu te čekanje potvrde od drugog čvora. Korisnici, to jest čvorovi, tada započinju potvrđivanje danog bloka. Ako blok nema netočnih podataka ni odstupanja, dobit će konsenzus od čvorova cijele mreže te biti spreman za pridruženje postojećem lancu blokova.

6. Ulančavanje novog bloka

Posljednji korak jest dodavanje bloka u lanac. Provjereni blok dobiva vremensku oznaku i dodaje se linearnim i kronološkim redom u lanac. Dodani blok emitira se cijeloj mreži i distribuira zbog izmjena za lokalno pohranjivanje javne knjige [10]. Rudar koji je stvorio dodani blok dobiva titulu pobjednika te biva financijski nagrađen.

3.3. Vrste i karakteristike blokova

Blokovi su osnovni gradivni elementi svakog lanca blokova. U prethodnom odjeljku govorili smo od čega se sastoji pojedini blok te kako se oni uklapaju u lanac. Sada ćemo reći nešto više o različitim tipovima blokova koji postoje. Kako postoje različiti tipovi arhitekture lanca blokova, tako postoje i različite vrste samih blokova u lancu. Razlikujemo tri vrste blokova u lancu.

Prvi blok (engl. *Genesis block*) predstavlja podrijetlo cijelog lanca. Prvi takav blok *izrudario* je Satoshi Nakamoto pri stvaranju Bitcoin lanca. To je temeljni blok te time omogućuje dodavanje novih blokova u lanac jer, kao što smo rekli, svaki blok se sastoji od adrese prethodnog bloka u lancu. Stablo kod kojeg svaki čvor sadrži adresu prethodnog bloka u stablu naziva se Merkleovo stablo. Merkleovo stablo, poznato i kao *hash* stablo, je struktura podataka čiji je svaki list označen s kriptografskim hash-em paketa podataka te čiji je svaki nadređeni čvor označen kriptografskim hash-em vrijednosti svojih podređenih [11].

Druga vrsta blokova su valjani blokovi (engl. *Valid blocks*). To su svi oni blokovi koji su dodani u lanac. Svaki takav blok sastoji se od niza transakcija koje se potvrđuju zajedno s blokom pa tako svaka transakcija u valjanom bloku postaje potvrđena transakcija. Svaki novi valjani blok dodan u lanac nastavlja potvrđivati ranije transakcije. To osigurava da je svaka transakcija i svaki blok u mreži potpuno siguran.

Treći, ujedno i posljednji, tip blokova u lancu su blokovi siročadi (engl. *Orphan blocks*). Ovi blokovi se rudare istovremeno s drugim blokom, ali ih lanac ne prihvaća. Može se dogodi da dva bloka imaju isti roditeljski blok. Tada samo jedan može biti prihvaćen u lanac. Mrežni blokovi odlučuju koji će se blok koristiti dopuštajući račvanje (engl. *fork*) između ta dva podređena bloka. Zatim, čvorovi određuju koji blok žele prihvatiti postizanjem validacijskog konsenzusa. Račvanje s više provjerenih blokova prihvaća se u lanac. Postupak provjere radi se pomoću PoW-a. Odbačeni blok naziva se blok siroče. Svi blokovi generirani iz bloka siročadi se vraćaju natrag u spremište memorije te čekaju nove rudare.

3.4. Kriptografija i enkripcija u lancu blokova

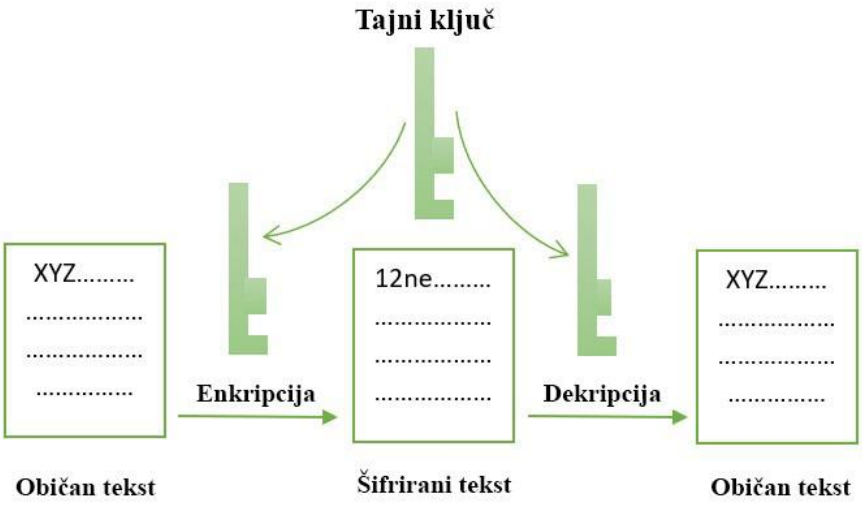
Riječ kriptografija proizlazi iz grčkih riječi Kryptos, što znači *sakriti* i Graphein, što znači *pisati*. Samo pošiljatelj i primatelj poruke mogu pristupiti sadržaju poruke putem sigurne komunikacijske metode poznate kao kriptografija. Pojam je usko povezan s enkripcijom, koja pretvara običan tekst u šifrirani tekst prije slanja i ponovno nakon primanja poruke. Kako je rečeno u [12], šifriranje je digitalni ekvivalent zaključavanja lokota, dok je dešifriranje digitalni ekvivalent otključavanja lokota.

Tehnologija lanca blokova kreirana je korištenjem raznih kriptografskih ideja. U lancu blokova kriptografija se uglavnom koristi za zaštitu privatnosti korisnika i informacija o transakcijama te za osiguravanje dosljednosti podataka. Osigurava da samo pojedinci kojima su podaci o transakciji namijenjeni mogu dobiti, pročitati i obraditi transakciju. Poznajemo dvije vrste kriptografije, simetričnim i asimetričnim ključem.

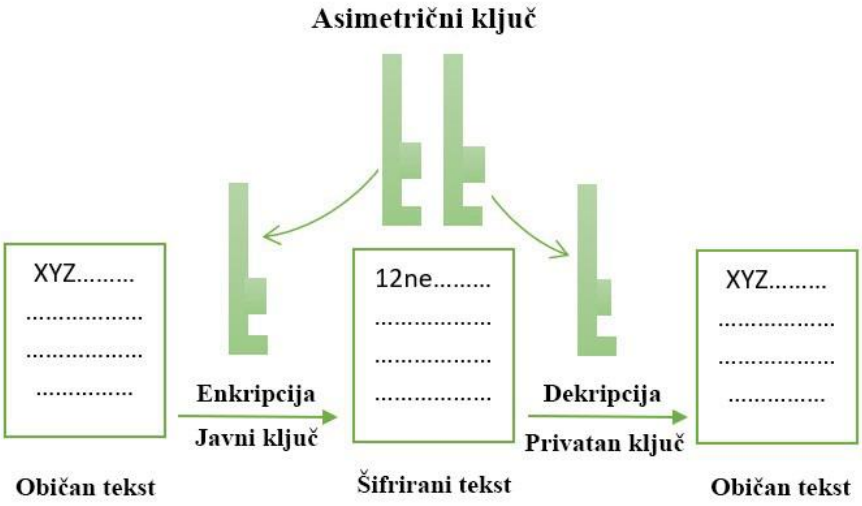
Kriptografija simetričnim (ili tajnim) ključem koristi isti ključ prilikom enkripcije i dekripcije. Samo osobe koje imaju tajni ključ mogu pristupiti poruci. Slika 3.2. prikazuje kriptografiju simetričnim ključem. Vidimo kako pošiljatelj šifrira običan tekst odgovarajućim ključem te taj ključ predaje primatelju koji pomoću njega dešifrira pošiljateljevu poruku.

Kriptografija asimetričnim (ili javnim) ključem koristi dvije vrste ključeva, javni i privatni. Radi na način da kada osoba želi poslati šifriranu poruku drugoj osobi, koristi javni ključ primatelja za enkripciju poruke. Zatim, primatelj koristi svoj privatni ključ za dekripciju poruke. Ovaj postupak omogućuje sigurnu komunikaciju bez potrebe za prethodnom razmjenom tajnog ključa između pošiljatelja i primatelja. Slika 3.3. prikazuje kriptografiju javnim ključem. Asimetrična kriptografija koristi digitalne potpise za verifikaciju. Svaku transakciju zabilježenu u bloku pošiljatelj potpisuje digitalnim potpisom i osigurava da nije došlo do gubitka podataka. Digitalni potpis je, poput stvarnog potpisa, postupak kojim se potvrđuje autentičnost i integritet podataka,

programske podrške ili digitalnih dokumenata, ali se koriste kriptografske ili matematičke tehnike koje su puno sigurnije od rukom pisanih potpisa. Digitalni potpis je način dokazivanja da poruka potječe od određene osobe, a ne od nekog drugog.



Slika 3.2. *Prikaz kriptografije simetričnim (tajnim) ključem*



Slika 3.3. *Prikaz kriptografije asimetričnim ključem*

Jedna od najznačajnijih upotreba kriptografije je kriptografsko raspršivanje (engl. *hashing*). Raspršivanje omogućuje nepromjenjivost u lancu blokova. Enkripcija u kriptografskom raspršivanju ne uključuje nikakvu potrebu za ključevima, bilo javnim ili privatnim nego uzima podatke te primjenom određenih algoritama generira izlaz koji se naziva *hash*. Bit hash-a je u tome

da uzima ulazne bitove beskonačne duljine, primjenjuje izračune te daje izlaze fiksne duljine. Ulazni podatak može biti bilo što, znak, rečenica, knjiga, datoteka, i drugo.

Važno je osvrnuti se na prednosti i ograničenja korištenja kriptografije u lancu blokova. Prednost je, kao što smo do sada govorili, enkripcija. Kriptografija koristi asimetričnu enkripciju ne bi li se osiguralo da transakcija štiti informacije i komunikaciju od neovlaštenog otkrivanja i pristupa informacijama. Također, kriptografija olakšava evidenciju transakcija pomoću enkripcije podataka, te pristupa podacima pomoću javnih i privatnih ključeva. Naposljetku, digitalni potpis sprječava sva neovlaštena tijela, to jest hakere, da mijenjaju podatke jer ukoliko dođe do promjene podataka, digitalni potpis postaje nevažeći.

Jedan od glavnih nedostataka korištenja kriptografije u lancu blokova je taj što snažno enkriptiranim i digitalno potpisanim informacijama može biti teško pristupiti čak i legitimnom korisniku. To može staviti u opasnost brzo donošenje odluka jer sustav treba proći sve zaštitne mjere. Kriptografija zahtijeva vremenska i novčana ulaganja. Kriptografija javnim ključem zahtijeva postavljanje i održavanje infrastrukture javnim ključem. Sigurnost kriptografskih tehnika ovisi o složenosti i težini matematičkog problema. Bilo kakav proboj u rješavanju tih problema može učiniti kriptografske tehnike ranjivima.

4. SIGURNOSNI RIZICI I NAPADI NA LANAC BLOKOVA

U ovom odjeljku detaljnije ćemo govoriti o sigurnosnim rizicima lanca blokova u pogledu napada. Objasnit ćemo najpopularnije vrste napada, opisati ih te dati pregled najvećih napada na lanac blokova do sada. Potom ćemo analizirati posljedice napada na sustav lanca blokova te dati primjere rješenja za sprječavanje takvih napada u budućnosti.

4.1. Napad 51%

Napad 51% je naziv za napad na lanac blokova od strane grupe rudara koji kontroliraju 51%, ili više, računalne snage za rješavanje kriptografskih zagonetki. Uspješni napadači dobivaju mogućnost blokiranja potvrđivanja novih transakcija kao i promjene redoslijeda novih transakcija. Mijenjanje blokova koji su dodani u lanac prije napada je vrlo teško, čak i u slučaju napada 51%. Što transakcije datiraju dalje u prošlost, to ih je sve teže promijeniti. Posjedovati 51% računalne snage znači da korisnik, organizacija, vlada, ili netko drugi, posjeduje više snage rudarenja od svih ostalih rudara u cijelom lancu zajedno (ostalih 49%).

Slika 4.1. prikazuje princip rada ovog napada. Napad se događa u nekoliko koraka. Prvo, entitet ili osoba zainteresirana za napad bi trebala postići dovoljno računalne snage da uspješno rudari blokove na kopiji lanca mreže u tajnosti. Kopija lanca se odvija paralelno s originalom. Stoga je ključ izvođenja napada 51% kupnja dovoljne količine računalne snage što zahtjeva velike količine resursa, odnosno novca. Ako zlonamjerni akter ne može financirati taj proces, napad se ne može dogoditi. Zbog svoje iznimne skupoće, vjerojatnost za ovakvim napada je vrlo mala.

Slika 4.1. *Principa rada napada 51%*

4.2. Problem dvostruke potrošnje

Problem dvostruke potrošnje (engl. *Double-spending problem*) je rizik da se kriptovaluta može koristiti dva ili više puta. Postavlja se pitanje, kako primatelj digitalnog novca može biti siguran da primljeni novac nije istovremeno poslan nekome drugom?

Do pojave pojma *dvostruka potrošna* dolazi uslijed digitalizacije novca. Fizički novac ne može biti dupliciran, to jest, valuta sa jedinstvenim serijskim brojem ne može biti na više mjesta od jednom.

Prema [13], problem dvostruke potrošnje znači da se dogodi više od jedne prijenosne radnje prije pravilnog ažuriranja na sustav lanca blokova. U slučaju kriptovalutnog sustava, ovaj napad se posebno odnosi na dvostruko trošenje bez ažuriranja stanja računa.

Kriptovaluta Bitcoin rješava ovaj problem na način da koristi decentraliziranu javnu knjigu kojoj mogu pristupiti svi korisnici sustava. Upravo taj javni pristup omogućuje svim korisnicima pregled povijesti transakcija te time osiguraju da njihov novac nije dvostruko potrošen. Slanje Bitcoin novčića dovodi do uništavanja pošiljateljevog novčića i kreiranja novog primateljevog novčića. Uništavanje novčića je zabilježeno i javno objavljeno ne bi li došlo do ponovnog slanja istog novčića, što bi dovelo do dvostruke potrošnje [14].

Napad 51%, o kojem smo više rekli u prethodnom potpoglavlju, usko je povezan s ovim napadom na način da ako neki entitet posjeduje 51%, ili više, cjelokupnog lanca, dobiva kontrolu nad verifikacijom transakcija i izgradnjom blokova u lancu. Tada zlonamjerni entitet može manipulirati mrežom na način da izvrše transakciju, a zatim izgrade paralelni lanac blokova u kojem ta transakcija ne postoji, što bi omogućilo dvostruku potrošnju.

4.3. Sybil napadi

Sybil napad je napad u kojem entitet ima brojne lažne identitete na lancu blokova iz zlonamjernih razloga. Ime je inspirirano knjigom iz 1973. godine pod nazivom Sybil. To je žena dijagnosticirana s disocijativnim poremećajem identiteta [15]. Dolazi do stvaranja velikog broja lažnih čvorova ne bi li se preuzela kontrola nad lancem. Postizanjem većinskih glasova u lancu, napadač može preuzeti kontrolu nad konsenzusom, to jest odlukama u mreži. Ovaj napad je moguć ako haker može preuzeti kontrolu nad višestrukim čvorovima tako da je žrtva okružena lažnim čvorovima koji zatvaraju sve njihove transakcije. Konačno, žrtva postaje otvorena za različite vrste napada s lažnim podacima [16]. Ovaj napad može pomoći u izvršavanju napada 51% na način da oštećuje integritet sustava lanca blokova.

Postoje razni načini sprječavanja Sybil napada. Jedan od tih načina je potvrda identiteta. Prema John Douceureru, postoji dva načina potvrde identiteta, izravno i neizravno. Izravno se odnosi na to da središnje tijelo provjerava i verificira svakog novog člana koji se pridruži mreži. Mogu se zahtijevati detalji kao što su IP adresa, ime, prezime, itd. Nedostatak ovog načina je taj što korisnik može dati netočne informacije. U neizravnom načinu, već provjereni članovi potvrđuju autentičnost novog budućeg člana. Osobni podaci nisu potrebni za pristup. Nedostatak ovog načina je taj što sustav može biti centraliziran, odnosno da provjereni članovi potvrđuju autentičnost novih članova koje poznaju, što je protiv decentralizirate prirode lanca blokova. Nadalje, postavljanje hijerarhijskog sustava igra značajnu ulogu u sprječavanju ovog napada. Dodani čvorovi u lanac će vjerojatno biti Sybil čvorovi te bi trebali biti stavljeni pod sumnju dok se ne potvrdi njihova autentičnost. Oni koji su u sustavu duže vrijeme trebaju imati ovlasti nad novopridošlicama. Ovo bi osiguralo prevenciju ovakve vrste napada na dodanim čvorova.

4.4. Krađa identiteta

Krađa identiteta (engl. *Phishing*) postaje sve češći oblik krađe osobnih podataka, kako u stvarnom svijetu, tako i u virtualnom. U kontekstu ovog rada, pojam se odnosi na vrstu kriptovalutne prijevare koja uključuje zavarivanje korisnika na način da korisnici odaju svoje privatne ključeve ili osobne informacije. Napadači se većinom *maskiraju* kao legitimno tijelo ne bi li stekli povjerenje korisnika sustava.

Napad započinje slanjem e-pošte (engl. *e-mail*) ili običnih poruka potencijalnim žrtvama. Te poruke većinom sadržavaju poveznice na lažne internet stranice koje izgledaju identično originalnim. Kada se korisnik prijavi na krivotvorenu stranicu, podaci mu bivaju ukradeni.

Postoje brojni primjeri ovakve vrste napada. *Napad kopljem* je ciljani napad usmjeren na određenu osobu ili organizaciju gdje napadač prethodno ima znanje o svojoj meti, što će iskoristiti prilikom prilagodbe e-pošte. Napad *lov na kitove* ima za cilj naštetiti pojedincima koji su na višim pozicijama unutar organizacija, na primjer direktorima. Opasniji je od prethodnog napada jer, ako, na primjer, direktor nasjedne na ovaj napad, može doći do raskola organizacije ili firme jer napadač ima pristup cijeloj mreži tvrtke. *Krađa identiteta putem SMS-a* koristi tekstualne poruke umjesto e-pošte. Kada žrtva klikne na poveznicu u poruci, biva preusmjerena na stranicu koja zahtijeva prijavu. Ukoliko žrtva pruži osobne podatke, napadač dobiva potpuni pristup nad računom žrtve.

Korisnik može pomoću samoedukacije izbjeći ovakvu vrstu napada. Postoje razni načini prepoznavanja krađe identiteta putem e-pošte; provjeriti vjerodostojnost stranice, gramatičke

pogreške, imena poveznica, provjeriti pošiljateljevu domenu e-pošte, koristiti autentifikaciju u dva koraka (engl. *two-factor authentication*), i drugi.

4.5. Pametni ugovori

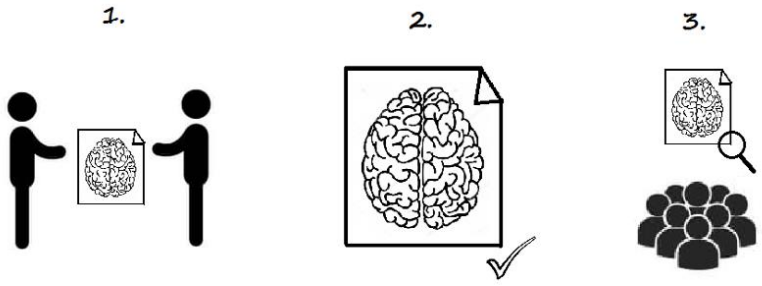
Prema [17], pametni ugovori (engl. *Smart contracts*) su jedna od mogućih i najperspektivnijih primjena tehnologije lanca blokova. Riječ *ugovor* se koristi jer imamo dvije strane koje prihvaćaju prethodno dogovorene uvjete te ako se ti uvjeti poštuju ugovor je na snazi. Kao i kod klasičnih ugovora, ako jedna strana prekrši prethodno dogovorene uvjete, ugovor se raskida te navedena firma snosi posljedice, bile one financijske ili neke druge.

Pametni ugovori su inačica ugovora kreirani na lancu blokova. Kod ovakve vrste ugovora eliminiraju se posrednici između dva entiteta pod ugovorom, kao što su banke, odvjetnici, i drugi. To su računalni programi koji se izvode kada je određeni uvjet zadovoljen na lancu. Zamisao je automatizirati i ubrzati proces donošenja sporazuma ne bi li svi sudionici sustava bili odmah sigurni, što bi dovelo do uštede vremena i eliminiranja treće strane.

Rade na način da imaju implementirane uvjete u lanac te samo čekaju okidač (engl. *trigger*), kao što su riječi *kada*, *ako*, *zatim*, i ostali uvjeti grananja. Unutar pametnog ugovora može postojati onoliko uvjeta koliko je potrebno da se sudionici uvjere da će zadatak biti obavljen na zadovoljavajući način. Da bi uspostavili uvjete, sudionici moraju odrediti kako su transakcije i njihovi podaci predstavljeni na lancu blokova, dogovoriti se o pravilima koja upravljaju tim transakcijama, istražiti sve moguće iznimke i definirati okvir za rješavanje sporova. Zatim, programer može programirati pametni ugovor, iako sve više organizacije koje koriste lanac blokova za poslovanje pružaju predloške, internet sučelja i druge alate na internetu zbog pojednostavljivanja strukturiranja pametnih ugovora.

Postoje mnoge prednosti korištenja pametnih ugovora kao što su brzina, učinkovitost i preciznost. Jednom kada je uvjet zadovoljen, ugovor se odmah izvršava. To se događa iz razloga što su pametni ugovori digitalni i automatizirani pa ne postoji gubitak vremena na papirologiju. Druga prednost je povjerenje i transparentnost. Pošto ne postoji posrednik i budući da se šifrirani zapisi o transakcijama dijele između korisnika, nema potrebe ispitivati jesu li informacije izmijenjene za osobnu korist. Nadalje, vrlo bitan faktor je sigurnost. Zapisi o transakcijama su šifrirani, što ih čini vrlo teškim za hakiranje. Budući da je svaki zapis povezan s prethodnim i sljedećim u lancu, to jest u javnoj knjizi, hakeri bi morali promijeniti cijeli lanac da bi promijenili jedan zapis.

Prema izvoru [18] postoje tri koraka prilikom kreiranja pametnog ugovora, prikazano na slici 4.2. Prvi korak je zapisivanje pravila razmjene dobara između dviju stranaka unutar programskog koda koji se pohranjuje u lanac blokova. Sadržaj ugovora dostupan je svim korisnicima sustava, dok stranke ostaju anonimne. Drugi korak nastupa nakon t*rigger eventa*[1] koji potiče izvršavanje pametnog ugovora prema dogovorenim pravilima. Treći korak dopušta ostalim korisnicima sustava da pretraže lanac blokova kako bi provjerili aktivnosti i rezultate definiranim ugovorom.



Slika 4.2. *Proces kreiranja pametnog ugovora*

4.6. Pregled najvećih napada na lanac blokova

U ovom potpoglavlju istražit ćemo najveće napade do sada u svijetu kriptovaluta, po pitanju ukradenog novca. U sljedećim potpoglavljima detaljnije ćemo analizirati svaki od ovih napada te dati primjere rješenja za sprječavanje takvih napada. Za potrebe analiziranja napada, koristit ćemo tablicu 4.1. koja prikazuje pet koraka analiziranja.

Analizirat ćemo najveće napade na Ethereum lanac blokova kao što su *TheDAO*, *prvi napad na Parity novčanik* i *Bitfinex*.

[1] *Trigger event* – događaj koji potiče pokretanje procesa

Tablica 4.1. *Koraci analize za niz pljački protiv sustava lanca blokova [19]*

Korak	Opis koraka	Kratak opis
1	Opisati prodiranje i opasnost sigurnosnog incidenta.	Ovaj korak opisuje prodiranje kibernetičkog napada i opasnost za Blockchain sustav. Kratak opis iskorištavanja i pljačke (engl. *heist*) uključen je u općeniti pregled.
2	Identificirati ograničenja i sigurnosne zahtjeve sustava.	Kako bi razumjeli sigurnosne zahtjeve, ovaj korak popisuje sva sigurnosna ograničenja sustava lanca blokova.
3	Identificirati sigurnosnu strukturu sustava kako bi se izbjegli kibernetički napadi.	Ovaj korak identificira i objašnjava strukturu obrane i zaštite u perspektivi sustava. Identifikacija uključuje ne samo sigurnost na razini sustava, već i zaštitu na razini koda.
4	Analizirati incident(e) hakiranja protiv sustava lanca blokova.	Ovaj korak započinje analizu iskorištavanja i hakiranja incidenta na sljedeći način: a) Neuspjesi sigurnosnih kontrolnih sustava. b) Neuspjesi u radu sustava. c) Neobrađene vanjske smetnje. d) Neuspjeh komunikacije / reakcije na incidente.
5	Identificirati proces odgovora na incidente i postupke za ublažavanje nakon kibernetičkog napada. Otkriti nedjelotvornost i nedostatke u pogledu sigurnosti sustava.	Ovaj korak ispituje koordinaciju / komunikaciju u strukturi sigurnosne kontrole i hijerarhiji u sustavu lanca blokova.

4.7. Analiza napada i posljedice

U ovom odjeljku detaljno ćemo analizirati napade, objasniti kako su izvedeni te navesti posljedice na lanac blokova.

4.7.1. TheDAO

Prisjetimo se, DAO ili decentralizirana autonomna organizacija je naziv za organizaciju vođenu na temelju koda na osnovu kojeg su se složili ljudi koji su pokrenuli DAO. Princip rada DAO-a je koristiti pametne ugovore što omogućuje samoodrživost i autonomnost sustava. Kao što velike kompanije imaju sastanke na kojima dioničari glasaju za odluke tvrtke koje kasnije glavni direktor pregledava, tako i DAO omogućuje svojim korisnicima da glasaju za odluke. Ako se donese zakon temeljen na odlukama, kod DAO-a se odmah mijenja. U svijetu kriptovaluta, DAO se može pokrenuti s određenim brojem tokena gdje svaki token predstavlja jedan glas. Onaj tko

ima najviše tokena ujedno ima i najviše moći. To upravo daje svakom tokenu vrijednost i upotrebljivost.

TheDAO je bila prva implementacija DAO-a temeljena na Ethereum lancu koju je stvorila njemačka tvrtka Slock.it [20]. Dvadeset tisuća ulagača je ukupno uložilo oko sto pedeset milijuna dolara u taj projekt. Račun projekta je hakiran te je pedeset milijuna dolara u Ethereum-u ukradeno. Zato danas poznajemo Ethereum Classic i obični Ethereum. Ethereum Classic je originalni lanac blokova koji je hakiran i pokraden, a Ethereum je zamišljen kao lanac blokova koji bi postepeno vraćao pokradeni novac. Ovaj potez se naziva račvanje.

Korak 1: Prodiranje i opasnost sigurnosnog incidenta

Nepoznati napadači iskoristili su sigurnosnu ranjivost u kodu poznatu kao rekurzivna pogreška. Ranjivost je omogućila napadaču da prenese sva sredstva s *DAO glavnog računa* na vlastiti [21]. Opasnost je bila u tome što je Ethereum lanac blokova dopustio nesigurnim decentraliziranim aplikacijama (engl. *dApps*) da rade na njegovom sustavu i sustav se nije adekvatno pobrinuo za mogući kibernetički napad.

Korak 2: Ograničenja i sigurnosni zahtjeva sustava [22]

- Ethereum lanac mora dopustiti decentraliziranim aplikacijama izvršavanje bez cenzure zbog načela *Kod je zakon*.
- TheDAO program mora proći temeljne sigurnosne provjere izvora ne bi li se smanjio rizik od incidenta povezanog s kibernetičkom sigurnosti.
- TheDAO program mora ispraviti sve poznate sigurnosne probleme prije nego se implementira na Ethereum lanac blokova.
- TheDAO mora razviti plan za odgovor na svaki kvar, neispravan rad ili kibernetički napad.
- TheDAO mora biti proaktivan za rješavanje svih problema koji se pojave.

Korak 3: Sigurnosna struktura sustava

Kao i ostali sustavi temeljeni na tehnologiji lanca blokova, Ethereum koristi sigurnosne značajke tehnologije lanca blokova kao ključnu i jedinu zaštitu sustava [23]. Slika 4.3. prikazuje pojednostavljenu shemu komunikacije između korisnika, decentraliziranih aplikacija i Ethereum lanca blokova. Kao što vidimo, čvor (korisnik) mora izvršiti autentifikaciju u Ethereum sustav prije nastavka s transakcijom ili pokretanjem decentraliziranih aplikacija unutar okruženja sustava. Međutim, Ethereum sustav strukturiran je na način da u potpunosti vjeruje svim odlukama i

izvršiteljima koje donosi softver (decentralizirane aplikacije) pokrenut na svakom čvoru bez validacije i verifikacije. Prema [24], prije TheDAO napada, Ethereum lanac nikada nije imao većih sigurnosnih problema poput programskih grešaka (engl. *bugs*) ili slično. Od njegovog pokretanja 2015. godine, radio je godinu dana bez ikakvih problema [25].

Nedugo nakon uspješnog prikupljanja sredstava za projekt TheDAO, pojavilo se mnogo pitanja u vezi sigurnosti sustava. Profesori informatike Gun Emin Turer i Vlad Zamfir iz Zaklade Ethereum su izvjestili zajednicu o potencijalnim sigurnosnim problemima u kodu. U njihovom radu [26] detaljnije je otkriveno kako su višestruki napadi manipulirali procesima što je, u konačnici, dovelo do ovog napada.

Slika 4.3. *Pojednostavljeni prikaz podatkovne komunikacije između čvora (korisnika), decentraliziranih aplikacija i Ethereum lanca blokova*

Korak 4: Analiza hakiranja

Napadač je uspješno izveo napad pronašavši dva *buga*[2] u funkciji *splitDAO* unutar TheDAO pametnog ugovora. Prvi se odnosio na rekurzivno pozivanje funkcije, a drugi na omogućavanje ažuriranja stanja računa žrtvinog pametnog ugovora.

Tjedan dana prije napada, Peter Vessenes, jedan od Ethereum programera, objavio je potencijalni problem u sustavu. Otkrio je sigurnosnu ranjivost u izvornom kodu (engl. *source code*) pametnog ugovora te je pružio detaljnu analizu i predložena rješenja. Glavni uzrok sigurnosnog problema bila je funkcija *splitDAO* u TheDAO pametnom ugovoru što je napadaču omogućilo rekurzivno pozivanje funkcije na ugovorima drugih korisnika s ciljem da iscrpi sredstva [27]. Zbog svoje prirode, funkcije pametnog ugovora Ethereum sustava mogu biti pokrenute i izvršene vanjskim zahtjevom. Ovime smo vidjeli kako se Ethereum-ovo pravilo "jedan ugovor može pokrenuti kod drugih ugovora" može zloupotrijebiti i pretvoriti u zlonamjerni napad [28].

[2] *Bug* – izraz koji se koristi za opisivanje greške ili neispravnosti u radu nekog softvera

Kod 4.1. prikazuje implementaciju TheDAO izvornog koda. Funkcija *splitDAO* omogućuje svojim korisnicima da stave određenu količinu sredstava za pojedini *_proposalID* [29]. Računa iznos sredstava koji se prenosi do osobe i potom poziva funkciju *createTokenProxy* za isplatu.

```
function splitDao (uint _proposalID, address _newCurator) noEther
onlyTokenholders returns (bool _success)
{
      // ...[snip]
       uint
fundsToBeMoved=(balances[msg.sender]*p.splitData[0].splitBalance)/
       p.splitData[0].totalSupply;
       if
(p.splitData[0].newDao.createTokenProxy.value(fundsToBeMoved)(msg.sender)
== false)
      {
            throw;
      }

        // ...[snip]
         Transfer(msg.sender, 0, balances[msg.sender]); // REDAK 1
         withdrawRewardFor(msg.sender);                 // REDAK 2
          totalSuppy -= balances[msg.sender];           // REDAK 3
          balances[msg.sender] = 0;                     // REDAK 4
          paidOut[msg.sender] = 0;                      // REDAK 5
          return true;
}
```

Kod 4.1. – *SplitDAO funkcija*

Prvi problem započinje u drugom retku koda (REDAK 2) gdje se poziva funkcija *withdrawRewardFor* kako je prikazano u kodu 4.2. Kada se funkcija pozove, vrijednosti *totalSupply* u trećem retku (REDAK 3), *balances* u četvrtom retku (REDAK 4) i *paidOut* u petom retku (REDAK 5) se ažuriraju, što dovodi do povlačenja sredstava [30].

Funkcija *withdrawRewardFor* je dio TheDAO pametnog ugovora koja omogućuje korisniku da zatraži povlačenje ulaganja iz ukupnog fonda, nazvano *split*. Problem je u samoj funkciji *withdrawRewardFor* jer kao parametar funkcije prima adresu primatelja podijeljenih sredstava pozivom vanjske funkcije. Također, funkcija se može pozivati rekurzivno, što znači da napadač može rekurzivno pozivati funkciju *splitDAO* te u parametre funkcije staviti adresu svojeg računa pa će tako sredstva biti prebačena na račun napadača [31].

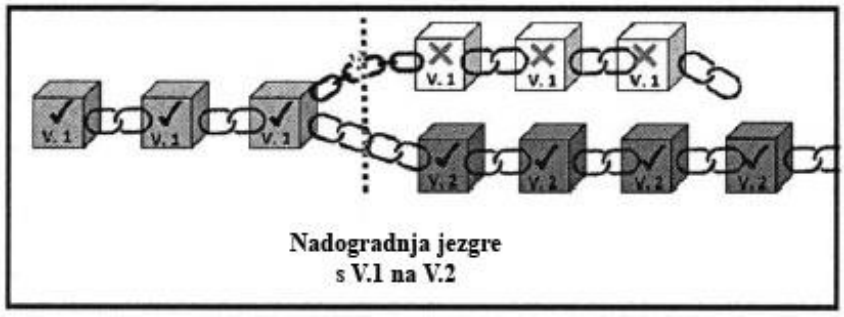
```
function withdrawRewardFor (address _account) noEther internal returns (bool
_success){
    // ...[snip]
    if (!rewardAccount.payOut(_account, reward)){
        throw;
    }
    paidOut[_account] += reward;
    return true;
}
```

Kod 4.2. – *withdrawRewardFor funkcija*

Korak 5: Odgovor na incidente i postupci za ublažavanje

Ethereum je održao konferenciju te omogućio svojim investitorima tri opcije [32] [33]:

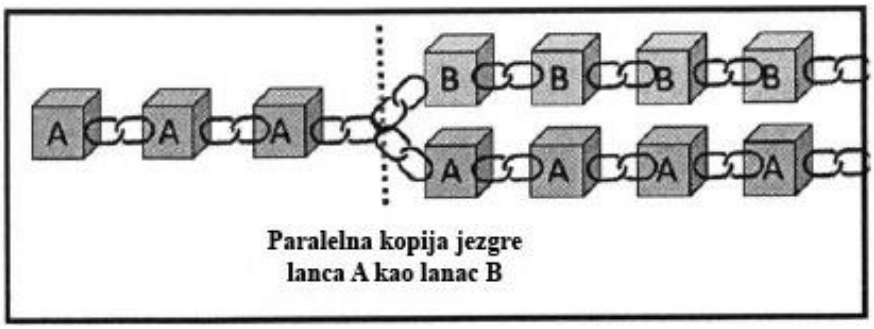
- Ne učiniti ništa: Ethereum lanac ostaje kakav je. Ništa se neće mijenjati niti prilagođavati. Napadač zadržava sav novac.
- Meko račvanje (engl. *soft fork*): Ovo će prepisati prethodne podatke u lanac blokova koristeći napad 51%. Kada novi lanac pređe 50% drugog lanca, novi lanac postaje glavni. Ovo bi rezultiralo gubitkom sredstava jer se kreira potpuno nova grana lanca. Proces mekog račvanja prikazan je slikom 4.4.



Slika 4.4. *Prikaz mekog račvanja*

- Tvrdo račvanje (engl. *hard fork*): Ovo će podijeliti postojeći lanac u dva dijela. Jedan će imati novi softverski protokol, a drugi će ostati na protokolu na kojem je bio kada se napad dogodio. Lanac blokova će poništiti transakcije koje su *izvukle* Ethereum za lanac koji je ostao kakav je bio prije račvanja. To će postići poništavanjem transakcija koje su drugi čvorovi (korisnici) potvrdili. Korisnici koji nisu bili napadnuti TheDAO

napadom trebali bi prijeći na novi softverski protokol. Tvrdo račvanje bi omogućilo svim žrtvama TheDAO napada povrat sredstava. Proces tvrdog račvanja prikazan je slikom 4.5.



Slika 4.5. *Prikaz tvrdog račvanja*

Prva odluka je bila koristiti meko račvanje no, neposredno prije primjene, došlo je do promjene na tvrdo račvanje jer su istraživači pronašli potencijalne prijetnje DoS (Denial of Service) u sustavu mekog račvanja [34]. Kao rezultat tvrdog račvanja, nastala su dva izolirana lanca blokova, Ethereum i Ethereum Classic koja koegzistiraju do danas.

4.7.2. Prvi napad na Parity novčanik

Kao što znamo, sustav lanca blokova temelji se na paru ključeva, javnih i privatnih. Ako korisnik ima privatan ključ koji odgovara adresi lanca blokova, on može promijeniti podatke na toj adresi. Problem je taj što sustav ima samo jednu provjeru autentičnosti, parove ključeva, te ako se ona zaobiđe sustav je vrlo ranjiv jer ga ne štiti ništa drugo.

Ne bi li se osigurala sigurnost ključa, osmišljena je aplikacija novčanik. Novčanik pohranjuje parove javnog i privatnog ključa korištenih u transakcijama na lancu. To i dalje nije u potpunosti sigurno jer iako preuzmemo novčanik na računalo, može doći do gubitka zbog hakiranja.

Kompanija BitGo je 2012. godine predstavila *Multi-Sig tehnologiju*[3] u nadi da riješi problem greške na jednom mjestu (engl. *single-point error*). Ova tehnologija je temeljena na novoj vrsti adrese nazvanom *Pay to Script Hash* (P2SH). Omogućuje pretvaranje jednog potpisa (privatnog ključa) u višestruke potpise i pohranjivanje istih na više strana, poput mobilnih uređaja ili online poslužitelja. Da bi došlo do transakcije, korisnik treba koristiti podskup ključeva (dva od tri privatna ključa) s više izvora (servera ili uređaja). Višestruki potpis osigurava sustavu lanca

[3] *Multi-Sig tehnologija* – tehnologija višestrukog potpisa. To je zahtjev da transakcija ima dva ili više potpisa, to jest provjera, prije nego što se može izvršiti. URL: https://www.techtarget.com/searchcio/definition/multisig-multisignature

blokova da može uspješno izvršiti transakciju iako je jedan od privatnih ključeva ukraden [35]. Suosnivač Ethereum lanca, Gavin Wood, pokrenuo je tehnologiju višestrukog potpisa na Ethereum lancu početkom 2017. godine te je ona smatrana jednom od najpovjerljivijih kriptovalutnih novčanika na tržištu prije pljačke [36].

Korak 1: Prodiranje i opasnost sigurnosnog incidenta

Nepoznati napadač iskoristio je nezaštićenu implementaciju novčanika s višestrukim potpisima koji radi na Ethereum lancu te je uspio ostvariti vlasništvo nad Ethereum novčanikom žrtve. Tri Ethereum *ICO*[4] projekta su bili žrtve pljačke što je rezultiralo gubitkom od oko sto pedeset i tri tisuće Ethereum-a u vrijednosti od trideset milijuna dolara. Opasnost je bila u tome što su nezaštićene decentralizirane aplikacije radile na Ethereum lancu bez dovoljnih sigurnosnih pregleda i provjera. Prvi napad na Parity novčanik uzrokovano je ne samo iskorištavanjem sigurnosne programske pogreške, već i nedostatkom kontrola sigurnosti i osiguranja rizika u sustavu lanca blokova.

Korak 2: Ograničenja i sigurnosni zahtjevi sustava

- Ethereum lanac mora dopustiti decentraliziranim aplikacijama izvršavanje bez cenzure zbog načela *Kod je zakon*.
- Novčanik s višestrukim potpisima mora proći temeljitu sigurnosnu provjeru izvornog koda kako bi se smanjio rizik od sigurnosnih incidenata u kibernetičkom sustavu.
- Novčanik s višestrukim potpisima mora ispraviti sve poznate sigurnosne probleme s dovoljnom provjerom ispravke prije implementacije u Ethereum-ov lanac blokova.
- Razvoj novčanika s višestrukim potpisima mora uključivati izradu plana za odgovor na incidente u slučaju kvarova, neispravnog rada ili kibernetičkih napada.

Korak 3: Sigurnosna struktura sustava

Dodavanje autentifikacije višestrukog potpisa u smislu sigurnosti sustava bio je siguran način za rješavanje pojedinačnih kvarova i osiguravanja visoke razine sigurnosti [37]. Međutim, problem je bio u tome što to rješenje zahtjeva veću potrošnju Ethereum-a. Kada se pametni ugovor implementira i izvršava, Ethereum-ov sustav lanca blokova naplaćuje malu količinu Ethereum-a, poznatiju kao *gas*. *Gas* se odnosi na vrijednost cijene potrebne za uspješno obavljanje transakcije ili izvršavanje ugovora na Ethereum-ovoj platformi [38].

[4] *ICO* – metoda stjecanja kapitala gdje kompanije prodaju ulagačima nove tokene ili kriptovalute. URL: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

S višestrukim potpisom, pametni ugovor mora pozvati funkciju(e) kako bi zaštitio prijenos podataka kada značajke ili metode pametnog ugovora komuniciraju s drugim pametnim ugovorima. Kao rezultat toga, implementacija višestrukog ugovora je sigurnija, ali i skuplja za izvođenje pametnih ugovora. Zbog tih dodatnih troškova 97% pametnih ugovora koji su se izvodili na Ethereum sustavu od studenog 2014. godine nisu koristili autentifikaciju višestrukog potpisa, već je bio potreban samo jedan ključ za autentifikaciju [39].

Kompanija Parity Technology riješila je problem troškova korištenjem zajedničkih biblioteka [40]. Parity Technology dijeli novčanik s višestrukim potpisima na dva ugovora: *WalletLibrary* ugovor koji se sastoji od funkcionalnosti višestrukog potpisa unutar biblioteke i ugovora koji ih poziva. U ovom slučaju, ako pametni ugovor uvozi funkcionalnost višestrukog potpisa iz unaprijed implementirane *WalletLibrary*, nema potrebe za dodatnim *gasom* za kasnije korištenje autentifikacije funkcionalnosti višestrukog potpisa [41].

Kod 4.3. prikazuje *WalletLibrary* ugovor. Varijabla *owner* predstavlja adresu vlasnika novčanika. Funkcija *initWallet* kao argumente prima adrese *_owners* (adrese vlasnika novčanika), *_required* (broj potrebnih potpisa za izvršavanje transakcije) i *_daylimit* (ograničenje dnevnog iznosa). Funkcija inicijalizira dnevno ograničenje pozivom funkcije *initDaylimit* i postavlja vlasnike novčanika pozivom funkcije *initMultiowned*. Detalji tih funkcija nisu prikazani u ovom kodu. Funkcija *changeOwner* prima adresu *_new_owner* kao argument te mijenja adresu vlasnika novčanika samo ako je pozvana od strane trenutnog vlasnika. Funkcija *withdraw* prima količinu novca koju vlasnik želi povući. Ova funkcija, također, provjerava je li pozvana od strane vlasnika novčanika i zatim šalje navedenu količinu novca vlasniku. Funkcija bez imena (engl. *fallback function*) je označena ključnom riječi *payable* te se koristi za prihvaćanje poslanih Ethereum-a. Ako je poslana vrijednost veća od nula, tada se koristi funkcija *delegatecall* za preusmjeravanje poziva na funkciju i omogućavanje izvršenja transakcije.

```
contract WalletLibrary
{
    address owner;
    // pozvan od strane konstruktora
    function initWallet(address[] _owners, uint _required, uint _daylimit){
        initDaylimit(_daylimit);
        initMultiowned(_owners, _required);
        // .... [snip]
    }
    function changeowner(address _new_owner) external{
        if (msg.sender == owner){
            owner = _new_owner;
        }
    }
    function () payable
    {
        if (msg.value > 0){
            Deposit(msg.sender, msg.value);
        }
        else if (msg.data.length > 0){
            _walletLibrary.delegatecall(msg.data);
        }
        // .... [snip]
    }
    function withdraw(uint amount) external returns (bool success){
        if (msg.sender == owner){
            return owner.send(amount);
        }
        else
            return false;
    }
}
```

Kod 4.3. – *WalletLibrary ugovor*

```
contract Wallet
{
    address constant _walletLibrary;
    address owner;
    // .... [snip]
    function Wallet(address _owner){
        _walletLibrary = Oxa657491cle7f16adb39b9b68e87bbb8d93988bc3;
        _walletLibrary.delegatecall(bytes4(sha3("initWallet(address)")),
_owner);
    }
    function withdraw(uint amount) returns (bool success){
        return  _walletLibrary.delegatecall(bytes4(sha3("withdraw(uint)")),
amount);
    }
    function () payable
    {
        if (msg.value > 0){
        Deposit(msg.sender, msg.value);
        }
        else if (msg.data.length > 0){
            _walletLibrary.delegatecall(msg.data);
        }
    }
    //....[snip]
}
```

Kod 4.4. – *Wallet ugovor*

Kod 4.4. prikazuje ugovor *Wallet*. Varijabla *_walletLibrary* sadrži adresu biblioteke (*WalletLibrary*). *Owner* predstavlja adresu vlasnika novčanika. U konstruktoru se predaje adresa vlasnika kao argument. Postavlja se vrijednost *_walletLibrary* na unaprijed određenu adresu te se koristi funkcija *delegatecall* za poziv funkcije *initWallet(address)* kako bi se inicijalizirao novčanik s proslijeđenim vlasnikom. Funkcija *withdraw* prima količinu novca koju vlasnik želi povući. Također, koristi *delegatecall* za poziv funkcije *withdraw(uint)* kako bi se izvršilo povlačenje sredstava. Funkcija označena ključnom riječi *payable* radi sve isto kao u prošlom

isječku koda. Ovaj dizajn je najvažniji faktor koji omogućuje novčaniku s višestrukim potpisima da minimizira potrošnju *gasa* putem višestruke potpisane autentifikacija na Ethereum lancu [42].

Korak 4: Analiza hakiranja

Napadači su kombinirali dva sigurnosna problema za uspješno izvođenje napada. Prvi se krije u delegirajućoj funkciji *payable*, unutar *Wallet* ugovora, koja vrši prijenos Ethereum-a. Međutim, ako transakcija ne sadrži Ethereum već samo podatke u sadržaju poruke, tada *Wallet* ugovor prosljeđuje poziv funkcije ugovoru *WalletLibrary*. Sve funkcije unutar *WalletLibrary* moraju biti javne jer se pozivaju iz ugovora pa zaključujemo da bilo koji pametni ugovor koji je u interakciji s *Wallet* ugovorom može pozivati funkcije u *WalletLibrary*.

Drugi problem je u funkciji *initWallet* ugovora *WalletLibrary*. Funkcija *initWallet* je konstruktor te se poziva prilikom kreiranja ugovora no što ako ju pokrenemo iz drugog pametnog ugovora koji je u interakciji s *Wallet* ugovorom? Ako se to dogodi, originalni vlasnik se može izmijeniti. Ovim načinom *Wallet* ugovor može biti pod kontrolom drugog korisnika.

Napad se odvijao u dva navrata. Prvi se odvio pozivanjem funkcije *initWallet* unutar *WalletLibrary* ugovora gdje napadač mijenja vlasnika ugovora [43]. Drugi napad poziva funkciju prijenosa sredstava za premještanje Ethereum-a na adresu napadača [44]. Prethodna funkcionalnost unutar *Wallet* ugovora kodirana je na način da se prvo verificira vlasnik te potom nastavi s izvršavanjem. Međutim, napadač je već promijenio podatke o vlasniku ugovora postavivši sebe kao vlasnika. Kombinacijom ova dva problema napadač je mogao uspješno pokrenuti sve javne funkcije iz biblioteke i prebaciti sva sredstva na svoju adresu.

Korak 5: Odgovor na incidente i postupci za ublažavanje

Pošto je decentralizacija ključ lanca blokova, ne možemo očekivati od nekog središnjeg tijela da djeluje na provale unutar lanca. Da se napad dogodi unutar centraliziranog sustava, mogli bismo očekivati brz i koncizan odgovor, u suprotnom ne. Nakon napada na Parity Technology, formirano je volontersko društvo programera nazvano *White Hack Group*. Odgovor je bio brz i točan te su uspješno prebacili preostale novčanike na njihove vlastite, jednako kao što je to učinio napadač. Zadržali su prebačene novčanike sve dok Parity Technology nije sanirala sigurnosni problem na Github-u [45]. Sačuvani novčanici su vraćeni korisnicima no ukradeni novac se nije mogao oporaviti.

Za razliku od slučaja TheDAO, ovdje se nije moglo izvršiti tvrdo račvanje zbog toga što je jako velik broja aktivnih pametnih ugovora još uvijek koristio Parity novčanike i jer nitko nije

mogao predvidjeti nuspojave na Ethereum sustav. Zajednica Ethereum programera odlučila je da neće izvršiti nikakvo račvanje jer bi to samo sustav izložilo dodatnim rizicima i ranjivostima, a vjerojatnost da se ukradena sredstva vrate su bila premala. Prema [46], povrata izgubljenih stvari nije bilo, a sredstva su trajno izgubljena.

4.7.3. Bitfinex pljačka

Bitfinex je platforma za trgovanje kriptovalutama koja je započela u Hong Kongu 2012. godine [47]. Do početka 2010. godine, transakcije kriptovalutama su se odvijale izvan lanca blokova (engl. *off-Blockchain*) i njima je upravljala središnja baza podataka. Bitfinex je prva mjenjačnica kriptovaluta koja je nudila transakcije na lancu blokova (engl. *on-Blockchain*), što je trgovanje kriptovalutama učinilo transparentnijim jer korisnici mogu provjeriti svoj novčanik u stvarnom vremenu [48]. U vrlo kratkom vremenu Bitfinex je postao jedna od najpopularnijih globalnih mjenjačnica kriptovaluta zbog svoje inovativnosti.

Bitfinex je pretrpio dva velika napada na sustav od 2015. do 2016. godine. Prvi se dogodio u svibnju 2015. godine, kada je ukradeno tisuću i petsto Bitcoin-a. Drugi se dogodio u kolovozu 2016. godine, kada je ukradeno sto dvadeset tisuća Bitcoin-a u vrijednosti od oko sedamdeset i dva milijuna dolara. Ovaj napad je zabilježen kao drugi najveći napad na sustav lanca blokova, s dvadeset milijuna dolara više od hakiranja TheDAO-a [49].

Korak 1: Prodiranje i opasnost sigurnosnog incidenta

Nepoznati napadač zaobišao je Bitfinex-ovu autentifikaciju s više potpisa (engl. *multi-signature authentication*) koju pruža tvrtka BitGo. Napadač je uspio ukloniti autentifikacijsku zaštitu i prebaciti sredstva s Bitfinex *skladišta* na svoj račun. Postojale su dvije opasnosti. Prva je bila ta što, prilikom izrade komponenti sustava i promjena konfiguracije u svrhu usklađivanja s propisima, Bitfinex nije sigurno uskladio komponente sustava što je dovelo sustav do ranjivosti. Drugi problem je bio u tome što je kompanija BitGo vodila sustav za autentifikaciju pa Bitfinex nije mogao brzo reagirati na napad.

Korak 2: Ograničenja i sigurnosni zahtjevi sustava [50]

- BitGo-ova odvojena implementacija višestrukog potpisa s Bitfinex-om mora provjeriti sigurnost prije potpisivanja bilo koje korisničke transakcije.
- BitGo-ova odvojena implementacija višestrukog potpisa s Bitfinex-om mora zaštititi nepoželjne zahtjeve za prijenos sredstava na kriptovalutni sustav lanca blokova.

- BitGo-ova odvojena implementacija višestrukog potpisa s Bitfinex-om mora surađivati s Bitgo-om i s više vlasnika kako bi smanjila rizik od krađe privatnih ključeva.
- Bitfinex i BitGo moraju komunicirati i surađivati jedni s drugim kako bi minimizirali sigurnosni rizik.

Korak 3: Sigurnosna struktura sustava

U svibnju 2015. godine, Bitfinex je izgubio oko tisuću i pet stotina Bitcoin-a. Bitfinex nije otkrio tehničke pojedinosti no uzrok je poznat; korištenje nesigurnih vrućih i hladnih novčanika [51]. Nakon incidenta, Bitfinex je odlučio implementirati dodatan sloj sigurnosnih komponenti sustava u suradnji s BitGo-om, koji pruža rješenje u obliku novčanika s višestrukim potpisima.

Kao što znamo, u sustavu lanca blokova, korisnik je identificiran na osnovu dva kriptografska podatka; javni i privatni ključ. Privatni ključ se koristi za autentifikaciju i autorizaciju transakcije, a javni ključ za dohvaćanje informacija o transakciji. BitGo-ov sustav radi na način da podijeli privatni ključ u tri dijela te ih pohrani na različitim mjestima [52]. Bitfinex jedan ključ pohranjuje na korisnikov vrući novčanik (engl. *hot wallet*)[5], a drugi pohranjuje na hladni novčanik (engl. *cold wallet*)[6]. BitGo čuva treći ključ kao način provjere korisnikove autorizacije. Prilikom transakcije, korisnik mora pružiti dva od tri moguća dijela ključa. Jedan će biti pružen ili korištenjem hladnog novčanika ili prijavom na Bitfinex koji će pružiti ključ iz vrućeg novčanika. Zadnji dio će pružiti BitGo kroz zasebnu prijavu [53].

Godinu dana kasnije *U.S. Commodity Futures Trading Commission (CFTC)* uvela je sankcije Bitfinex-u kaznivši ih s sedamdeset i pet tisuća dolara zbog ilegalnih financijskih transakcija izvan burze [54]. Zatim je Bitfinex premjestio sredstva na vruće skladište (engl. *hot storage*) koje je bilo na internetu.

Korak 4: Analiza hakiranja

Napadač je prvo provalio u Bitfinex-ovu platformu kako bi dobio jedan dio privatnog ključa za žrtve. Nije poznato kako je došlo do ovoga jer Bitfinex nije objavio svoje tehničke pojedinosti. Iako Bitfinex nije otkrio točne pojedinosti, napadač je uspio dobiti pristup izvornom kodu i informacijama za pokretanje programa izravno na BitGo-ov server za autentifikaciju kako bi potpisao sve zahtjeve za transakcije. BitGo pruža mogućnost pokretanja funkcija u obliku javne

[5] *Vrući novčanik* – kriptovalutni novčanik povezan s internetom.
[6] *Hladni novčanik* – kriptovalutni novčanik koji nije povezan s internetom.

biblioteke za svoje korisnike. U svrhu testiranja, programeri koriste tu funkcionalnost pružanjem ključa za autentifikaciju. Konačna verzija koda ne bi trebala sadržavati informacije o biblioteci i vrijednosti ključa. Međutim, te informacije su ostale u izvornom kodu pa je napadač samo s jednim ključem mogao ući u sustav pozivajući javne funkcije BitGo-ove biblioteke [55].

Ne treba cijelu krivnju staviti na Bitfinex. BitGo i CFTC su također zaslužni za sigurnosne propuste zbog kojih se napad dogodio. Bitfinex nije sigurno implementirao integraciju BitGo-a i nije proveo sigurnosnu reviziju promjena u sustavu. Nadalje, BitGo nije uspio provjeriti sigurnosnu implementaciju pa nije bio u mogućnosti signalizirati velik broj transakcija. Također, CTFC snosi krivnju zbog zatraženih promjena u sustavu. Bitfinex je postavio alarm na BitGo-ov server u slučaju velikog broja transakcija u kratkom vremenu kako bi minimizirao napad no alarm nije funkcionirao zbog nepoznatih razloga [56].

Korak 5: Odgovor na incidente i postupci za ublažavanje

Nakon napada, Bitfinex je objavio suspenziju BitGo-ovog novčanika s višestrukim potpisima. Bitfinex je uspio otkloniti dva uzroka pljače: mogućnost korištenja BitGo-ove biblioteke te zaobilaženje sustava upozorenja za prijenos podataka. Također, Bitfinex je objavio ponovnu implementaciju višestrukog potpisa i uspostavu sigurnih opcija za pohranu kriptovaluta [57].

5. MJERE SIGURNOSTI LANCA BLOKOVA

U ovom odjeljku govorit ćemo o mjerama sigurnosti za sprječavanje ponovnih napada u budućnosti. Osvrnut ćemo se na tehničke, organizacijske i pravne mjere za jačanje sigurnosti lanca blokova.

5.1. Tehničke mjere za jačanje sigurnosti lanca blokova

U pogledu tehničkih mjera za jačanje sigurnosti lanca blokova, govorit ćemo o nekim od mogućih mjera kao što su osiguravanje anonimnosti, identifikacija i autentifikacija te redovito ažuriranje i nadogradnja.

Svaki korisnik unutar lanca blokova ima dodijeljenu jedinstvenu adresu i koristi kriptografsku vrijednost (javni ključ) zbog osiguravanja anonimnosti. Dokazano je da algoritam koji stvara privatni i javni ključ nije moguće odgonetnuti te se time garantira anonimnost korisnika. Bilo bi bolje da sustav pruža pseudonimnost umjesto anonimnosti. Pseudonimnost je metoda korištena za pomutnju identiteta osobe ili grupe [58]. Anonimnost znači da ne postoji mogućnost praćenja identiteta osobe ili grupe, ali korisnik i dalje mora pružiti identifikacijske informacije za interakciju sa sustavom.

Identifikacija i autentifikacija glavni su faktori prilikom validiranja korisnika u sustavu. Jedna od mogućih mjera je korištenje dvofaktorske autentifikacije. Tradicionalna autentifikacija temelji se na samo jednom faktoru, obično korisničkom imenu i lozinki. Dodavanjem dvofaktorske autentifikacije bi se osigurao dodatan sloj sigurnosti za provjeru identiteta korisnika. Ovime bi se osigurala zaštita korisničkih novčanika, platformi za trgovanje kriptovalutama ili drugih aplikacija unutar sustava lanca blokova na način da bi korisnik morao generirati lozinku putem aplikacije te je unijeti u sustav. Sustav bi tada pružio poboljšane mjere sigurnosti, smanjenje rizika od krađe identiteta te povećanje pouzdanosti korisnika.

Redovito ažuriranje i zakrpe igraju ključnu ulogu u jačanju sigurnosti lanca blokova. To su važne mjere koje se primjenjuju kako bi se održao integritet i zaštita sustava lanca blokova od sigurnosnih rizika i ranjivosti. Redovito ažuriranje odnosi se na praksu nadogradnje softverskih komponenti i protokola lanca blokova na najnovije verzije. Redovito ažuriranje omogućuje razvojnim timovima da reagiraju brzo na propuste i pruže validno rješenje za dani problem. Svaki sustav koji se redovito ne ažurira otvoren je za potencijalne napade jer, kao što smo to vidjeli iz dosadašnjih primjera napada, napadači su u stanju vrlo brzo uvidjeti problem u izvornom kodu i to iskoristiti u svoju korist.

5.2. Organizacijske mjere za jačanje sigurnosti lanca blokova

Organizacijske mjere osvrću se na obuku i svijest korisnika, politike sigurnosti i kontrolu pristupa. Detaljnije ćemo reći o svakoj stavci u ovom potpoglavlju.

Obuka i edukacija zaposlenika ključan je faktor u sustavu lanca blokova. S obzirom na složenost i specifičnosti tehnologije, važno je educirati korisnike o sigurnosnim praksama i postupcima kako bi se smanjio rizik od sigurnosnih prijetnji i pogrešaka. Korisnici koji su prošli obuku će biti kvalificiraniji za otklanjanje sigurnosnih propusta unutar sustava.

Glavni cilj politike sigurnosti je osigurati zaštitu podataka, smanjiti rizik od sigurnosnih prijetnji te osigurati dosljednost i usklađenost s pravilima i propisima. Politika sigurnosti treba definirati pravila pristupa informacijskom sustavu temeljenom na lancu blokova. To uključuje definiranje razina pristupa, autorizacije i autentifikacije korisnika te upravljanje korisničkim privilegijama. Pravila pristupa trebaju biti jasno definirana kako bi se osiguralo da samo ovlaštene osobe imaju pristup podacima i funkcionalnostima lanca blokova.

Kontrola pristupa se odnosi na uspostavljanje sustava i postupaka koji kontroliraju pristup informacijskom sustavu temeljenom na tehnologiji lanca blokova. Cilj kontrole pristupa je osigurati da samo ovlaštene osobe imaju pristup podacima i funkcionalnostima lanca blokova, dok se neovlašteni pristup sprječava. Kontrola pristupa uključuje upravljanje korisničkim računima i pravima pristupa te primjenu dvofaktorske autentifikacije.

5.3. Pravne mjere za jačanje sigurnosti lanca blokova

Pravne mjere su ključne za osiguravanje povjerenja, transparentnosti i integriteta, kako u stvarnom svijetu, tako i u digitalnom. Neki od ključnih aspekata pravnih mjera su reguliranje digitalnih valuta, odgovornost i kaznene mjere te međunarodna suradnja.

Pravne mjere trebaju regulirati korištenje, trgovanje i upravljanje digitalnim valutama kako bi se spriječile prijevare, pranje novca ili slične protuzakonite mjere. Pošto kriptovalute poput Bitcoin-a i Ethereum-a postaju sve popularnije, javlja se potreba za regulacijom istih. Također, ovo može biti usmjereno na očuvanje financijske stabilnosti što može uključivati pravila o kapitalnim zahtjevima za tvrtke koje se bave kriptovalutama. Regulacija ima za cilj zaštititi potrošače od prijevara ili nepoštivanja ugovora. To može uključivati pravila o transparentnosti, informiranju potrošača o rizicima, jasnim uvjetima korištenja i pravilima za rješavanje sporova.

Pravne mjere trebaju jasno definirati odgovornosti sudionika u lancu blokova i propisati kaznene mjere za zloupotrebu, neovlašteni pristup, krađu identiteta i druge sigurnosne prijetnje.

Propisivanje kaznenih mjera je nužno jer ukoliko korisnik prekrši neki od pravnih aspekata, treba biti sankcioniran. To može uključivati novčane kazne, zatvorske kazne ili druge sankcije koje su propisane zakonom. Ovo se ne odnosi samo na korisnika već i na organizacije koje se bave poslovanjem digitalnim novcem.

Međunarodna suradnja se odnosi na međunarodne sporazume i suradnju između država što zahtjeva razmjenu informacija koja treba biti regulirana. Države bi trebale međusobno surađivati ukoliko otkriju sigurnosne prijetnje ili potencijalne prijevare unutar sustava. Također, neophodno je razviti međunarodne standarde koji se odnose na sigurnosne protokole, pravila zaštite podataka, identifikaciju i autentifikaciju. Važno je napomenuti kako su otvorena međunarodna komunikacija, dijeljenje informacija i usklađivanje propisa ključ uspjeha u postizanju sigurnog i pouzdanog okruženja za lanac blokova na međunarodnoj razini.

6. ZAKLJUČAK

U ovom završnom radu govorili smo o sustavu lanca blokova i njegovom načinu rada, proučili sigurnosne rizike, istražili najveće napade te dali primjere poboljšanja u cilju sprječavanja ponovnih napada. Tehnologija lanca blokova široko je zastupljena u današnjem svijetu poslovanja te pokriva razne sektore omogućavajući brzu i laku razmjenu dobara. Međutim, kao i svaka tehnologija, lanac blokova nosi određene sigurnosne izazove i rizike. Posebnu pažnju treba pridodati sigurnosti sustava s kojim obavljamo transakcije te ovaj rad može pomoći pri razumijevanju i potencijalnom izlaganju mogućim rizicima. Kao što smo imali priliku vidjeti, sve i najmanji propust u izvornom kodu lanca blokova može dovesti do kolapsa sustava.

Kombinacija različitih mjera za poboljšanje sigurnosti lanca blokova pridonosi jačanju sustava, stvarajući pouzdanu i sigurnu infrastrukturu za transakcije i razmjenu podataka. Važno je kontinuirano nadograđivati i poboljšavati sigurnosne mehanizme kako bi se odgovorilo na nove, potencijalne, prijetnje i izazove te osiguralo povjerenje sudionika u lancu blokova.

Ova inovativna tehnologija ima potencijal pružiti brojne prednosti različitim sektorima i globalnoj ekonomiji, unapređujući transparentnost, smanjujući rizik od prijevara te poboljšavajući efikasnost transakcijskih procesa. Uz kontinuirano unapređivanje i održavanje, moguće je izgraditi stabilan i pouzdan ekosustav lanca blokova koji će pružiti brojne prednosti različitim sektorima i globalnoj ekonomiji.

LITERATURA

[1] Božena Dević, KRIPTOVALUTE, Repozitorij Elektrotehničkog fakulteta Osijek, Osijek, 2018., dostupno na: https://repozitorij.efst.unist.hr/islandora/object/efst%3A2288/datastream/PDF/view [Pristupljeno 23.05.2023.]

[2] M. Gupta, Blockchain for Dummies, IBM, John Wiley & Sons, Inc., Hoboken, New York, 2017

[3] Reiff, N., rujan 2022., Investopedia. URL: https://www.investopedia.com/tech/what-dao/ Decentralizirana Autonomna Organizacija: Definicija, Uloga, i primjer / Decentralized Autonomous Organization: Definition, Purpose, and Example

[4] Bitcoin.it, „the Bitcoin Wiki“, bitcoin.it, 14.04.2010. [Online], dostupno na: https://en.bitcoin.it/wiki/Main Page. [Pristupljeno 23.05.2023.]

[5] Neven Travaš, PRIMJENA BLOCKCHAINA I PAMETNIH UGOVORA, Repozitorij Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, Zagreb, 2018., dostupno na: https://repozitorij.foi.unizg.hr/islandora/object/foi%3A4419/datastream/PDF/view [Pristupljeno 23.05.2023.]

[6] Bandara, K., Y., 2021., End-to-End Tracing and Congestion in a Blockchain: A Supply Chain Use Case in Hyperledger Fabric, Nacionalno sveučilište Galway, Irska

[7] Unocoin, „Bitcoin miners vs Bitcoin nodes“, Unocoin, 6.02.2018. [Online], dostupno na: https://blog.unocoin.com/bitcoin-miners-vs-bitcoin-nodes-6a4d35be9712. [Pristupljeno 23.05.2023.]

[8] G. Greenspan, „The Blockchain Immutability Myth“, Coindesk, 09 05 2017. [Online], dostupno na: https://www.coindesk.com/blockchain-immutability-myth/. [Pristupljeno 23.05.2023.]

[9] B. Wiki, “Proof of work“, [Online], dostupno na: https://en.bitcoin.it/wiki/Proofofwork. [Pristupljeno 23.05.2023.]

[10] N. C. Fabien Aepli, „Blockchain simply explained“, Mangeat, 2017.

[11] „Merkle tree“, https://en.wikipedia.org/wiki/Merkle_tree. [Pristupljeno 23.05.2023.]

[12] D. Drescher, Blockchain Basic – A Non-Tehnical Introduction in 25 Steps, Apress, Frankfurt am Main, Njemačka, 2017.

[13] J. Frankenfield, „Double-Spending“, Investopedia, 5 7 2018. [Online], dostupno na: https://www.investopedia.com/terms/d/doublespending.asp [Pristupljeno 23.05.2023.]

[14] Anonymus, veljača 2023., River Financial. URL: https://river.com/learn/what-is-the-double-spend-problem Što je problem dvostruke potrošnje? / What Is the Double Spend Problem?

[15] Neary, L., listopad 2011., Prava 'Sybil' priznaje da su višestruke osobnosti lažne. [Pristupljeno 23.05.2023.]

[16] Aprorit, „Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology“, Aprorit, [Online], dostupno na: https://www.apriorit.com/dev-blog/578-blockchain-attackvectors. [Pristupljeno 23.05.2023.].

[17] Voras, I., Što su pametni ugovori – uvod, UBIK, 2018., dostupno na:: https://ubik.hr/2018/03/26/sto-su-pametni-ugovori-uvod/ [Pristupljeno 23.05.2023.].

[18] Smart Contracts: The Blockchain Technology That Will Replace Lawyers: What are Smart Contracts, Blockgeeks Inc., 2016., dostupno na: https://blockgeeks.com/guides/smart-contracts/ [Pristupljeno 23.05.2023.].

[19] S. M. Hamid Salim, „Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks“, u Composite Information Systems Laboratory (CISL), Boston, 2014. [Pristupljeno 23.05.2023.].

[20] T. K. Sharma, „Details Of The Dao Hacking In Ethereum In 2016“, Blockchain Council, 20 8 2017. [Online]. Dostupno na: https://www.blockchaincouncil.org/blockchain/details-of-the-dao-hacking-in-ethereum-in-2016/. [Pristupljeno 23.05.2023.].

[21] M. d. Castillo, „Cornell Professor Calls for 'DAO 2.0' Movement“, 22 6 2016. [Online]. Dostupno na: https://www.coindesk.com/cornell-prof-discovered-dao-vulnerabilityreveals- IO-exploits/. [Pristupljeno 23.05.2023.].

[22] G. Greenspan, „Smart contracts and the DAO implosion“, 22 6 2016. [Online], dostupno na: https://www.multichain.com/blog/2016/06/smart-contracts-the-daoimplosion/. [Pristupljeno 23.05.2023.].

[23] L. Mearian, „How blockchain will underpin the new trust economy“, 7 12 2017. [Online], dostupno na: https://www.computerworld.com/article/3240906/security/howblockchain- will-underpin-the-new-trust-economy.html. [Pristupljeno 23.05.2023.].

[24] L. Coleman, „DAO Vulnerability Raises Questions of Trust and the Human Factor“, 24 6 2016. [Online], dostupno na: https://www.ccn.com/dao-vulnerability-trust-humanfactor/. [Pristupljeno 23.05.2023.].

[25] D. Siegel, „Understanding The DAO Hack for Journalists“, 17 6 2016. [Online], dostupno na: https://medium.com/@pullnews/understanding-the-dao-hack-for-joumalists- 2312dd43e993. [Pristupljeno 23.05.2023.].

[26] V. Z. E. G. S. Dino Mark, „A Call for a Temporary Moratorium on „The DAO““, 30 5 2016. [Online], dostupno na: https://docs.google.com/document/d/1OkTyCmGPhvZy94F7VWySdQ4lsBacR2dUgGTtV98C40. [Pristupljeno 23.05.2023.].

[27] P. Vessenes, „More Ethereum Attacks: Race-To-Empty is the Real Deal“, Vessenes Blog, 9 6 2016. [Online], dostupno na: https://vessenes.com/more-ethereum-attacks-raceto-empty-is-the-real-deal/. [Pristupljeno 23.05.2023.].

[28] M. P. G. Gelvez, „Explaining the DAO exploit for beginners in Solidity“, Medium, 16 10 2016. [Online], dostupno na: https://medium.com/@MyPaoG/explaining-the-daoexploit-for-beginners-in-solidity-80ee84f0d470. [Pristupljeno 23.05.2023.].

[29] K. R, „The Dao Hack And Recursive Calling Vulnerability In Ethereum“, What is Ethereum Organization, 5 8 2017. [Online], dostupno na:https://what-isethereum.org/2017/08/05/the-dao-hack-and-recursive-calling-vulnerability-inethereum.[Pristupljeno 23.05.2023.].

[30] P. Daian, „Analysis of the DAO exploit“, Hacking Distributed, 18 6 2016. [Online], dostupno na: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/.[Pristupljeno 23.05.2023.].

[31] R. Graham, „Ethereum/TheDAO hack simplified“, Errata Security, 18 6 2016. [Online]. Dostupno na: https://blog.erratasec.com/2016/06/etheriumdao-hacksimilfied.html#.WOQQei2ZPUK. [Pristupljeno 02.06.2023.].

[32] Investopedia, „Hard Fork“, Investopedia, [Online], dostupno na: https://www.investopedia.com/terms/h/hard-fork.asp#ixzz5E8ZcLqLR. [Pristupljeno 02.06.2023.].

[33] CryptoGraphics, „Hard and Soft Fork“, [Online], dostupno na: https://cryptographics.info/cryptographics/blockchain/hard-soft-forks/. [Pristupljeno 02.06.2023.].

[34] V. Zamfir, „The DAO Hard Fork, and the Negotiation that Couldn't Happen“, Medium, 19 7 2016. [Online], dostupno na: https://medium.com/@VladZamfir/the-dao-hard-forkand-the-negotiation-that-couldnt-happen-bdd2aedefe84. [Pristupljeno 02.06.2023.].

[35] C. Aventinus, „Parity Multisig Wallet Hacked, or How Come?“, Coin Telegraph, 13 11 2017. [Online], dostupno na: https://cointelegraph.com/news/parity-multisig-wallethacked-or-how-come. [Pristupljeno 03.06.2023.].

[36] S. Schroeder, „Not again: Hackers steal $52 million worth of Ethereum“, Mashable, 20 7 2017. [Online], dostupno na: https://mashable.com/2017/07/20/ethereum-hackers-theft-32-million/#JPX2TL5fgZq9. [Pristupljeno 03.06.2023.].

[37] B. Chan, „How Ethereum's Wallets Are Evolving“, Coin Desk, 17 9 2016. [Online], dostupno na: https://www.coindesk.com/ethereums-wallets-evolving/. [Pristupljeno 03.06.2023.].

[38] Investopedia, „Gas (Ethereum)“, Investopedia, [Online], dostupno na: https://www.investopedia.com/terms/g/gas-ethereum.asp. [Pristupljeno 03.06.2023.].

[39] B. Davenport, „What is Multi-Sig, and What Can It Do?“, Coin Center, 11 2015. [Online], dostupno na: https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do. [Pristupljeno 03.06.2023.].

[40] C. Reitwiessner, „Smart Contract Security“, Ethereum Blog, 10 6 2016. [Online], dostupno na: https://blog.ethereum.org/2016/06/10/smart-contract-security/. [Pristupljeno 03.06.2023.].

[41] H. Qureshi, „A hacker stole $31 M of Ether-how it happened, and what it means for Ethereum“, 20 7 2017. [Online]. Dostupno na: https://medium.freecodecamp.org/a-hackerstole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e3 3ce. [Pristupljeno 03.06.2023.].

[42] D. J. a. G. S. Lorenz Breidenbach, „An In-Depth Look at the Parity Multisig Bug“, Hacking Distributed, 22 7 2017. [Online], dostupno na: http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/. [Pristupljeno 03.06.2023.].

[43] Etherscan, „Transactions::Adresa: 0x9dbf0326a03a2a3719c27be4fa69aacc9857fd23Ia8d9dcaede4bb083def75ec“, Etherscan, 19 7 2017. [Online], dostupno na: https://etherscan.io/tx/Ox9dbfD326aO3a2a3719c27be4fa69aacc9857fd231a8d9dcaede4bb083def75ec. [Pristupljeno 03.06.2023.].

[44] Etherscan, „Transactions::Adresa: OxeeflOfc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c“, Etherscan, 19 7 2017. [Online], dostupno na: https://etherscan.io/tx/OxeeflOfc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c. [Pristupljeno 03.06.2023.].

[45] Gavofyork, „Fix initialisation bug. (#6102)“, Parity Technology, 19 7 2017. [Online], dostupno na: https://github.com/paritytech/parityethereum/commit/b640df8fbb964da7538eef268dffc125b081a82f. [Pristupljeno 03.06.2023.].

[46] C. Masters, „Ethereum Hard Fork Explained“, Cryptovest, 11 8 2017. [Online], dostupno na: https://cryptovest.com/education/ethereum-hard-fork-explained/. [Pristupljeno 03.06.2023.].

[47] Wikipedia, „Bitfinex“, Wikipedia, [Online], dostupno na: https://en.wikipedia.org/wiki/Bitfinex. [Pristupljeno 04.06.2023.].

[48] Y. B. Perez, „Bitfinex First Bitcoin Exchange to Offer On-Blockchain Transactions“, Coin Desk, 4 6 2015. [Online], dostupno na: https://www.coindesk.com/bitfinex-bitcoinexchange-on-blockchain-transactions/. [Pristupljeno 04.06.2023.].

[49] B. B. Exchange, „Bitfinex.com Review - Scam or Not?“, Best Bitcoin Exchange, [Online], dostupno na: http://www.bestbitcoinexchange.net/en/bitfinex-com/. [Pristupljeno 04.06.2023.].

[50] J. I. Wong, „Bitcoin exchanges can't stop getting hacked, no matter what security system they use“, QZ, 4 8 2016. [Online], dostupno na: https://qz.com/749789/bitcoinexchanges-cant-stop-getting-hacked-no-matter-what-security-system-they-use/. [Pristupljeno 04.06.2023.].

[51] J. Maxim, „Bitfinex Hot Wallets Hacked, More Than 1,400 Bitcoin May Be Stolen“, Bitcoin Magazine, 22 5 2015. [Online], dostupno na:

https://bitcoinmagazine.com/articles/bitfinex-hot-wallets-hacked- 1 400-bitcoin-maystolen-1432326539/. [Pristupljeno 04.06.2023.].

[52] S. Higgins, „The Bitfinex Bitcoin Hack: What We Know (And Don't Know)“, CoinDesk, 3 8 2016. [Online], dostupno na:
https://www.coindesk.com/bitfinex-bitcoin-hackknow-dont-know/. [Pristupljeno 04.06.2023.].

[53] A. Hayes, „You've been Buttfinessed“, Bitmex, 6 8 2016. [Online], dostupno na:
https://blog.bitmex.com/youve-been-buttfinessed/. [Pristupljeno 04.06.2023.].

[54] D. Shares, „CFTC fines bitcoin exchange Bitfinex $75,000 for illegal off-exchange financial transactions“, Bitcoin.com, 2 6 2016. [Online], dostupno na:
https://news.bitcoin.com/cftc-fines-bitcoin-exchange-bitfinex-75000-illegal-offexchange-financial-transactions/. [Pristupljeno 04.06.2023.].

[55] L. P. Adrian Shedden, „The impact of the Bitfinex hack on cryptocurrencies“, Cyber Security Law & Practice, no. Sept, pp. 7-9, 2016.

[56] pitchbend, „How was Bitfinex hacked!? Users need to know“, Reddit, 19 11 2017. [Online], dostupno na:
https://www.reddit.com/r/BitcoinMarkets/comments/5dn784/howwasbitfinexhacked_usersneedtoknow/. [Pristupljeno 04.06.2023.].

[57] Z. Tackett, „Bitfinex: Update Regarding Security Audit, Financial Audit, And More“, Bitfinex, 17 8 2016. [Online], dostupno na:
https://www.reddit.com/r/BitcoinMarkets/comments/4y4uwl/bitfinex-update-regarding_securityaudit/. [Pristupljeno 04.06.2023.].

[58] M. Taylor, „Bitcoin Isn't Anonymous, and That's Ok“, Coin Central, 25 6 2018. [Online], dostupno na:
https://coincentral.com/bitcoin-isnt-anonymous-and-thats-ok/. [Pristupljeno 10.06.2023.].

SAŽETAK

Zadatak završnog rada je upoznati se sa sustavom lanca blokova i njegovom sigurnosti. Detaljno je objašnjen princip rada i opisani su neki od mogućih napada na sustav. Kroz primjere napada, dan je detaljan pregled utjecaja sigurnosti lanca blokova na obavljanje transakcija te kako propusti unutar sustava mogu negativno utjecati na povjerenje i sigurnost korisnika. Tijekom analize napada na lanac blokova uočili smo da je ova tehnologija sigurna no postoje izazovi i ranjivosti s kojim se suočava. U cilju poboljšanja sigurnosti sustava, dane su mjere za jačanje sigurnosti lanca blokova.

Uz sve izazove i sigurnosne rizike, lanac blokova i dalje pokazuje potencijal i primjenu u različitim sektorima. Primjeri korištenja lanca blokova u praksi svjedoče o inovativnosti i mogućnostima koje ova tehnologija pruža u stvaranju sigurnijeg, transparentnijeg i efikasnijeg poslovnog okruženja. Ova tehnologija ima velik potencijal za transformaciju različitih industrija. Međutim, kako bismo iskoristili sve prednosti koje nudi, ključno je kontinuirano ulaganje u sigurnost i razvoj odgovarajućih sigurnosnih mjera.

Rezultat je cjelovit pregled sigurnosti sustava lanca blokova te prednosti i nedostaci korištenja istog.

Ključne riječi: dekripcija, enkripcija, lanac blokova, napadi, pametni ugovori, prednosti i nedostatci, sigurnost lanca blokova, transakcija.

ABSTRACT

Blockchain security

The task of the final paper is to familiarize oneself with the blockchain system and its security. The working principle is explained in detail, and some possible attacks on the system are described. Through examples of attacks, a detailed overview of the impact of blockchain security on transaction execution is provided, as well as how vulnerabilities within the system can negatively affect user trust and security. During the analysis of blockchain attacks, it was observed that this technology is secure, but it faces challenges and vulnerabilities. In order to enhance the security of the system, measures to strengthen the security of the blockchain are presented.

Despite all the challenges and security risks, blockchain continues to demostrate potential and application in various sectors. Examples of real-world blockchain usage attest to the innovation and possibilities that this technology offers in creating a more secure, transparent and efficient business environment. This technology has a great potential to transform different industries. However, in order to harness al the advantages it offers, it is crucial to continuously invest in security and develop appropriate security measures.

The result is a comprehensive overview of the security of blockchain systems, along with the advantages and disadvantages of using them.

Keywords: decryption, encryption, blockchain, attacks, smart contracts, advantages and disadvantages, blockchain security, transaction.

ŽIVOTOPIS

Marin Šimundić, rođen je u Puli, Republika Hrvatska, 20. listopada 2001. godine kao jedino dijete roditelja Maria i Marijane. U Nuštru završava osnovnu školu (Osnovna škola Zrinskih Nuštar), a u Vinkovcima opću gimnaziju (Gimnazija Matije Antuna Reljkovića). Pohađao je školu stranih jezika u Vinkovcima te ostvarivao brojna sportska dostignuća u svijetu stolnog tenisa. Godine 2020. upisuje Fakultet elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, smjer računarstvo – računalni inženjer.

Vlastoručni potpis

_____

Marin Šimundić