Detekcija nepravilnosti i analiza transakcija na Ethereum mreži

Jana Botkuljak

Sadržaj

1 Uvod

1.1 O bazi podataka

U ovom završnom praktičnom projektu analizira se skup podataka o transakcijama na Ethereum blockchainu s ciljem otkrivanja čimbenika povezanih sa sumnjivim aktivnostima. Korišten je javno dostupni skup podataka s platforme Kaggle, konkretno iz analize *Fraud Detection in Ethereum Transactions*. Ovi podaci korišteni su i u sklopu šireg istraživanja o detekciji prevara u kontekstu pametnih ugovora i decentraliziranih financija (*DeFi*).

Skup podataka obuhvaća 9841 adresu i 51 varijablu po računu, uključujući broj transakcija, količine poslanog i primljenog Ethera, aktivnosti na pametnim ugovorima, broj jedinstvenih adresa, razne metrike učestalosti i vremenskih obrazaca, kao i binarnu oznaku *FLAG* koja ukazuje je li neka adresa označena kao prevarantska.

Osim navedenog skupa, korišten je i Etherscan API za dohvat dodatnih informacija o transakcijama, uključujući detaljne podatke o vremenskom slijedu, iznosima i potrošnji gas-a (naknada koju korisnici plaćaju za izvršavanje transakcija i pametnih ugovora na Ethereum mreži), što je omogućilo dublju analizu ponašanja pojedinih adresa. Prije primjene metoda za detekciju anomalija kao što je Benfordov zakon, provedena je detaljna analiza odnosa između odabranih varijabli i oznake prevare kako bi se razumjeli obrasci ponašanja koji karakteriziraju sumnjive aktivnosti.

U početnom dijelu istraživanja obrađeni su sljedeći odnosi i obrasci:

- Jesu li velike transakcije povezane s prevarama?
- Je li ukupan broj poslanih transakcija povezan s prevarama?
- Kako učestalost slanja transakcija korelira s prevarantskim ponašanjem?
- Jesu li računi koji šalju velik broj transakcija male vrijednosti češće označeni kao sumnjivi?
- Koliki je broj jedinstvenih adresa kojima računi šalju transakcije i postoji li povezanost s oznakom *FLAG*?
- Statističko testiranje razlika između sumnjivih i nesumnjivih adresa
- Korelacijska analiza između ključnih kvantitativnih varijabli (*total.ether.received, total.ether.sent,* total.ether.balance)
- Izrada i analiza logističkog regresijskog modela za klasifikaciju računa.

Cilj ove analize bio je steći dublji uvid u obrasce ponašanja sumnjivih adresa te identificirati metrike koje mogu služiti kao prediktori prevare. Time se stvorila osnova za primjenu Benfordovog zakona i drugih metoda za detekciju anomalija koje mogu dodatno osnažiti zaključke o prevarantskim aktivnostima na blockchainu.

1.2 Općenito o detekciji prevara u pametnim ugovorima i DeFi-u

Prevara u pametnim ugovorima i decentraliziranim financijama (*DeFi*) predstavlja ozbiljan problem koji nastaje kada zlonamjerne osobe iskoriste ranjivosti u kodu ili mehanizmima financijskih aplikacija temeljenih na blockchain tehnologiji. Pametni ugovori su računalni programi koji automatski izvršavaju uvjete ugovora, a njihova sigurnost i pouzdanost ključne su za očuvanje povjerenja korisnika.

Prevare u ovom kontekstu mogu uključivati manipulacije transakcijama, krađu sredstava, lažne prikaze likvidnosti, *pump and dump* sheme ili iskorištavanje bugova u kodu. Budući da su DeFi protokoli međusobno povezani, prevare se često šire kroz više platformi, što povećava opseg i težinu nastale štete.

Rizici se dodatno povećavaju zbog složenosti pametnih ugovora, nedostatka institucionalne regulacije i anonimnosti korisnika. Iako je tehnologija blockchaina transparentna, sofisticirane metode prikrivanja identiteta i aktivnosti čine detekciju prevarantskog ponašanja izazovnom.

U okviru ovog istraživanja naglasak će biti na analizi stvarnih transakcijskih podataka u svrhu prepoznavanja obrazaca koji ukazuju na prevaru. Kroz kombinaciju statističkih metoda i tehnika za detekciju anomalija, uključujući Benfordov zakon, razmatraju se mogućnosti rane identifikacije sumnjivih računa i povećanja sigurnosti DeFi sustava.

1.3 Opis varijabli

Baza sadrži 9841 zapisa i 51 varijablu. Svaki zapis odnosi se na jednu adresu na blockchainu s podacima o transakcijama i tokenima.

X - Redni broj zapisa

Tip: kvantitativna diskretna varijabla

Index - Identifikator zapisa

Tip: kvantitativna diskretna varijabla

FLAG - Statusna oznaka (0 ili 1), označava prevaru ili ne

Tip: kvalitativna nominalna varijabla

Avg.min.between.sent.txn - Prosječno vrijeme u minutama između poslanih transakcija

Tip: kvantitativna kontinuirana varijabla

Avg.min.between.received.txn - Prosječno vrijeme između primljenih transakcija

Tip: kvantitativna kontinuirana varijabla

Time.Diff.between.first.and.last.Mins - Ukupno vrijeme u minutama između prve i zadnje transakcije

Tip: kvantitativna kontinuirana varijabla

Sent.tnx - Broj poslanih transakcija

Tip: kvantitativna diskretna varijabla

Received.Tnx - Broj primljenih transakcija

Tip: kvantitativna diskretna varijabla

Unique.Received.From.Addresses - Broj jedinstvenih adresa s kojih su primljene transakcije

Tip: kvantitativna diskretna varijabla

Unique.Sent.To.Addresses - Broj jedinstvenih adresa kojima su slane transakcije

Tip: kvantitativna diskretna varijabla

min.value.received - Minimalna primljena vrijednost u jednoj transakciji

Tip: kvantitativna kontinuirana varijabla

max.value.received - Maksimalna primljena vrijednost u jednoj transakciji

Tip: kvantitativna kontinuirana varijabla

avg.val.received - Prosječna primljena vrijednost u svim transakcijama

Tip: kvantitativna kontinuirana varijabla

min.val.sent - Minimalna poslana vrijednost u jednoj transakciji

Tip: kvantitativna kontinuirana varijabla

max.val.sent - Maksimalna poslana vrijednost u jednoj transakciji

Tip: kvantitativna kontinuirana varijabla

avg.val.sent - Prosječna poslana vrijednost u svim transakcijama

Tip: kvantitativna kontinuirana varijabla

total.transactions.including.tnx.to.create.contract - Ukupan broj transakcija uključujući kreiranje ugovora

Tip: kvantitativna diskretna varijabla

total.Ether.sent - Ukupno Etera poslana s adrese

Tip: kvantitativna kontinuirana varijabla

total.ether.received - Ukupna količina Etera primljena na adresu

Tip: kvantitativna kontinuirana varijabla

total.ether.balance - Trenutno stanje Ethera na adresi (primljeno – poslano)

Tip: kvantitativna kontinuirana varijabla

2 Analiza podataka

2.1 Jesu li velike transakcije povezane s prevarama?

Pogledajmo distribuciju računa prema prisutnosti velikih transakcija, prikazanu u *Tablici 1.* U ovoj analizi, najprije je postavljen prag koji klasificira određene transakcije kao velike. Račun je klasificiran kao račun s velikom transakcijom ako njegova najveća transakcija prelazi vrijednost koja je veća od 90% svih ostalih transakcija.

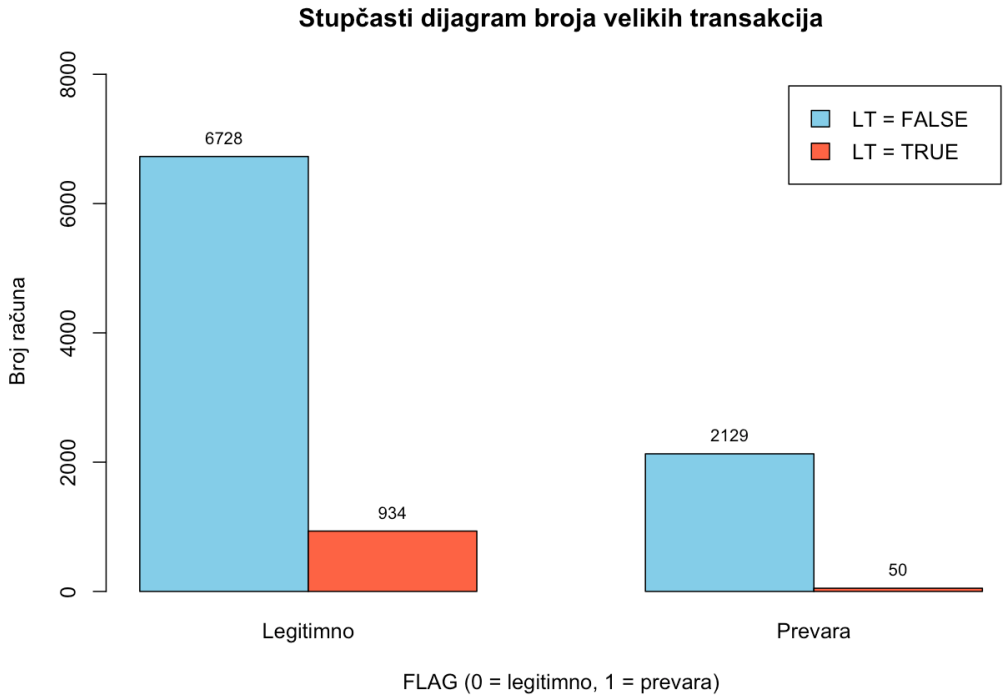
Large_Transaction	FLAG = 0 (legitimni)	FLAG = 1 (prevarni)	Ukupno
FALSE	2845	901	3746
TRUE	935	49	984

Tablica 1: Frekvencijska tablica velikih transakcija prema tipu računa

Rezultati prikazuju zanimljiv, ali iznenađujući obrazac. Naime, računi s velikim transakcijama ($LT = TRUE$) većinom su legitimni - njih čak 935 od ukupno 984 (odnosno 94.92%). Suprotno tome, samo 5.08% računa koji su izvršili veliku transakciju su označeni kao prevarni.

S druge strane, među računima bez velikih transakcija ($LT = FALSE$), čak 24.04% su prevare, dok je 75.96% legitimnih. Ova razlika u udjelima između dvije grupe otkriva zanimljiv kontrast - velika transakcija, iako potencijalno sumnjiva po veličini, nije karakteristika prevarnih računa. Dapače, prevare su znatno češće u slučajevima gdje nije zabilježena velika transakcija.

Empirijska distribucija prikazana stupčastim dijagramom (*Prikaz 1*) grafički prikazuje rezultate iz tablice. Uočljivo je da je broj prevarnih računa značajno veći među onima koji nemaju veliku transakciju, dok su računi s velikim transakcijama gotovo u potpunosti legitimni. Vizualna razlika u visini stupaca omogućuje lakšu usporedbu i jasno ilustrira kako velike transakcije nisu indikator prevare, što je važno pri izgradnji sustava za otkrivanje prevara.



Prikaz 1: Stupčasti dijagram broja velikih transakcija - usporedba računa prema prisutnosti velikih transakcija

Analiza sugerira da su velike transakcije sigurnije nego što se na prvi pogled čini. Prevaranti češće izbjegavaju velike iznose, vjerojatno kako bi ostali neprimijećeni. Stoga, u analizi sumnjivog ponašanja treba se fokusirati na obrasce ponašanja, a ne samo na iznos transakcije. Promatranje učestalosti, vremena između transakcija i kombinacija faktora vjerojatno će pružiti dublji uvid u prevarne aktivnosti.

2.2 Je li ukupan broj poslanih transakcija povezan s prevarama?

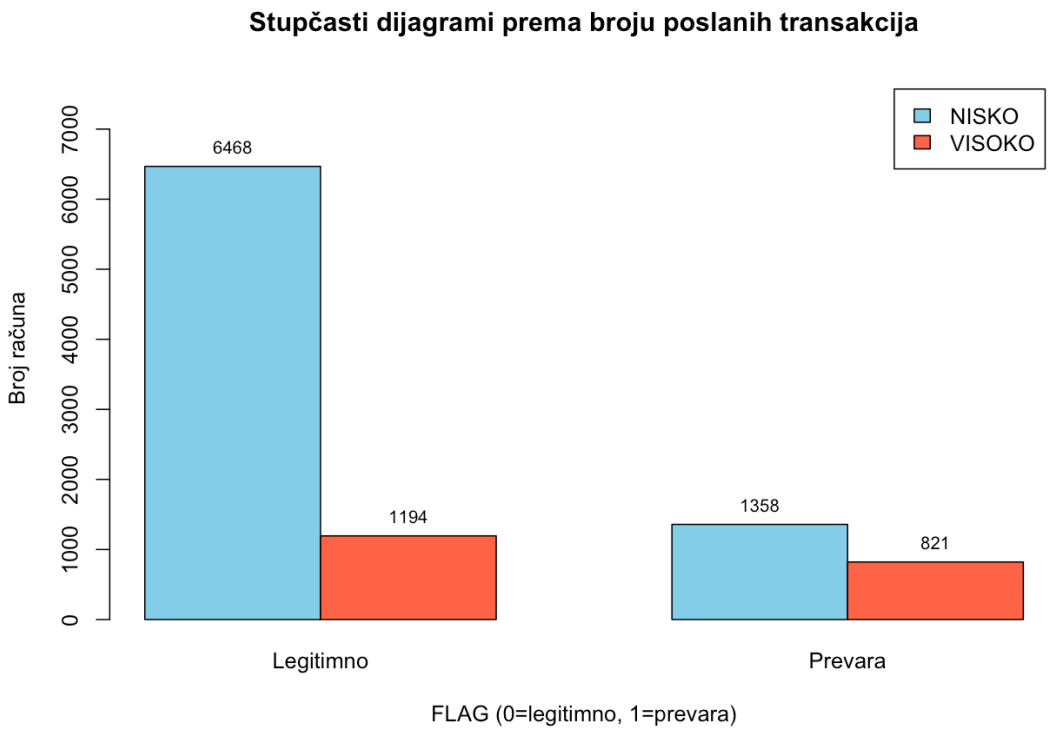
Analiza se temelji na ukupnom broju poslanih transakcija po računu, jer on pruža značajan uvid u korisničko ponašanje. Računi s vrlo malim brojem transakcija češće pripadaju prevarantskim korisnicima, dok legitimni korisnici obično šalju veći i stabilniji broj transakcija tijekom vremena.

Postavljen je prag koji dijeli račune na nisku i visoku aktivnost. Prema *Tablici 2*, gotovo 41% računa s niskom aktivnošću pripada prevarantskim, dok je među računima s visokom aktivnošću udio prevara oko 17%.

Low_Sent_Tnx	FLAG = 0 (Legitimno)	FLAG = 1 (Prevara)
FALSE	82,65	17,35
TRUE	59,26	40,74

Tablica 2: Relativne frekvencije (%) prevarantskih i legitimnih računa prema aktivnosti u broju poslanih transakcija

Prikaz 2 ilustrira razliku u broju legitimnih i prevarantskih računa između ovih dviju grupa. Rezultati pokazuju da računi s malim brojem transakcija imaju veću vjerojatnost prevarantskog ponašanja, što potvrđuje da broj poslanih transakcija može biti koristan indikator sumnjivih aktivnosti.

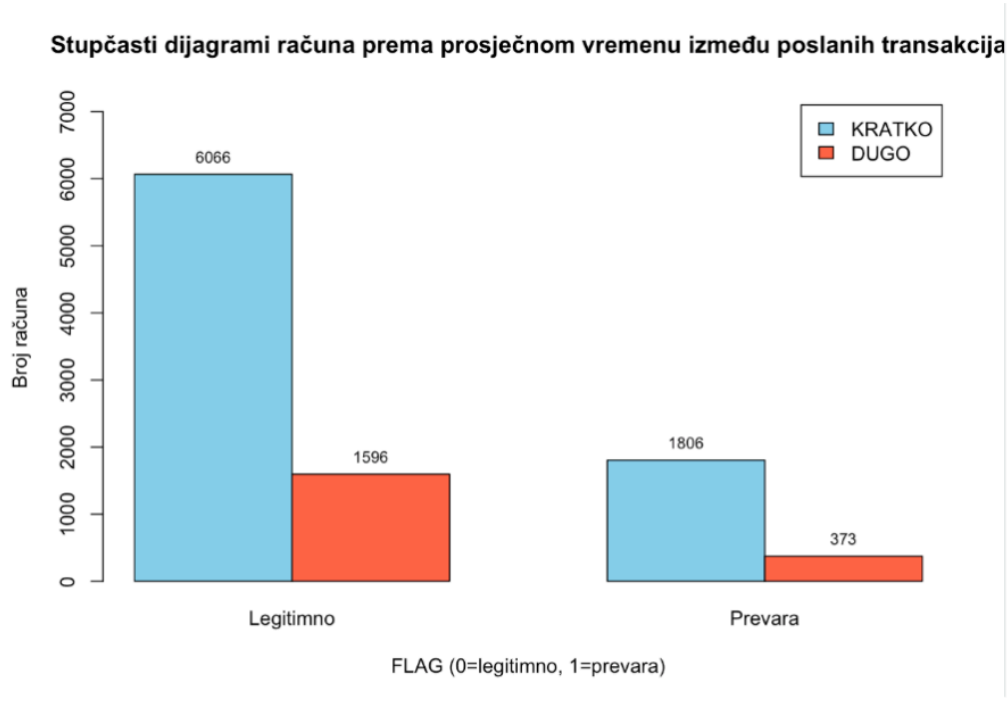


Prikaz 2: Stupčasti dijagrami računa prema broju poslanih transakcija (niska vs. visoka aktivnost)

2.3 Učestalost slanja transakcija i njezina povezanost s prevarantskim ponašanjem

Varijabla prosječnog vremena između poslanih transakcija može otkriti obrasce korisničkog ponašanja – računi s vrlo kratkim intervalima često ukazuju na automatizirano ili sumnjivo ponašanje, dok legitimni korisnici šalju transakcije u prirodnijim razmacima.

Uveden je prag koji dijeli račune prema kratkim i dugim intervalima između transakcija. Rezultati *(Prikaz 3)* pokazuju da 23% računa s kratkim intervalima pripada prevarantskim, a među računima s dužim intervalima udio je 19%.

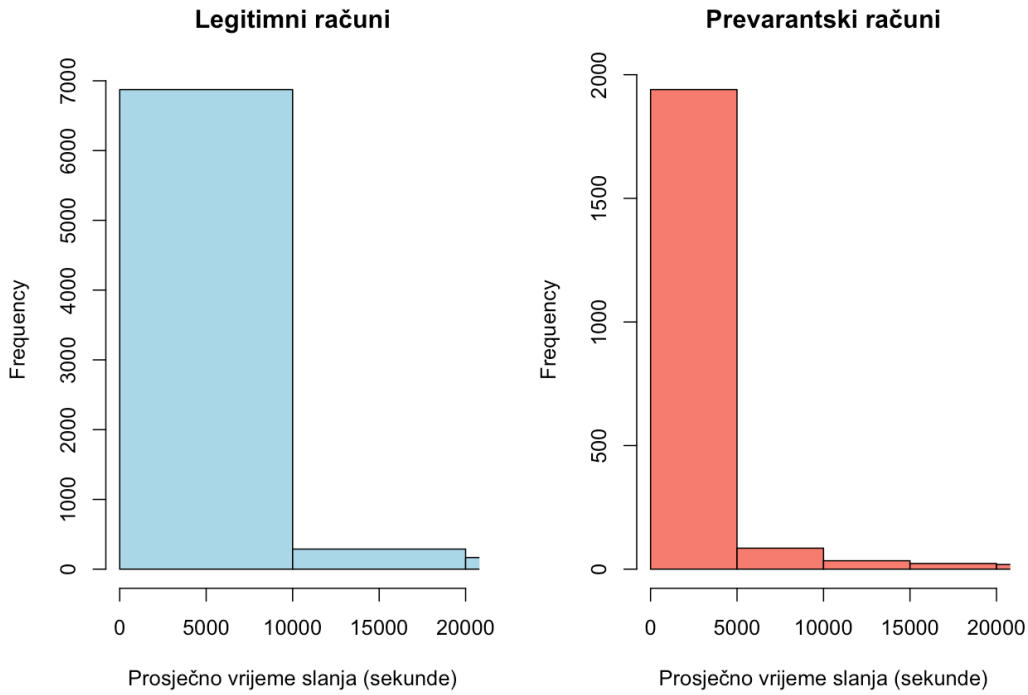


Prikaz 3: Stupčasti dijagrami računa prema prosječnom vremenu između poslanih transakcija (kratki vs. dugi intervali)

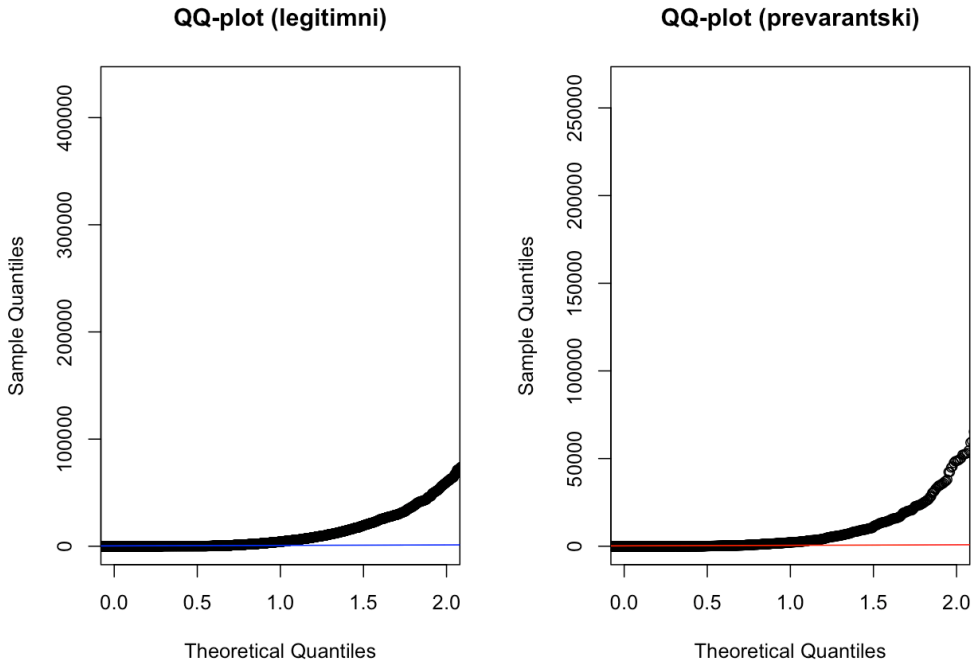
Za formalnu provjeru povezanosti korišten je χ^2 test nezavisnosti, gdje je nultom hipotezom pretpostavljena nezavisnost prosječnog vremena između transakcija i oznake računa ($FLAG$). Budući da je p-vrijednost značajno manja od 0.05, odbacujemo H_0 i potvrđujemo statistički značajnu povezanost.

Daljnja analiza empirijskih distribucija unutar skupina *(Prikazi 4 i 5)* pokazuje izraženu asimetričnost i veliki broj ekstremnih vrijednosti, što upućuje na ne-normalnu distribuciju. Stoga je za usporedbu grupa korišten neparametarski Mann-Whitney-Wilcoxon test (MWW), koji ne zahtijeva normalnost podataka, ali uspoređuje medijane između dviju skupina. No,

budući da distribucije nisu istog oblika rezultat interpretiramo šire: Test pokazuje razliku u distribucijama (ne nužno i u medijanima).

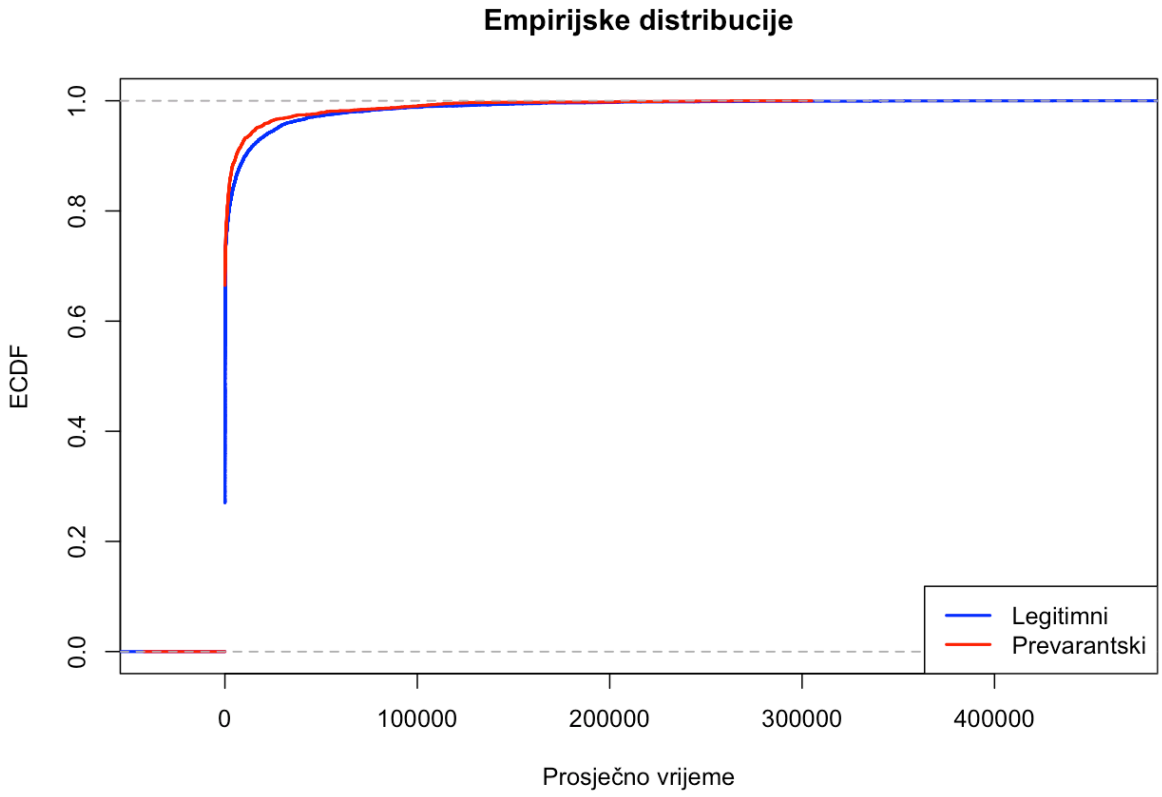


Prikaz 4: Histogram distribucije prosječnog vremena između transakcija za legitimne i prevarantske račune – prikaz asimetrije i ekstremnih vrijednosti



Prikaz 5: Q-Q dijagram usporedbe distribucije prosječnog vremena između transakcija legitimnih i prevarantskih računa – provjera odstupanja od normalnosti

Test je pokazao izrazito statistički značajnu razliku ($p < 2.2e\text{-}16$), potvrđujući da legitimni i prevarantski računi značajno razlikuju u vremenskim intervalima između transakcija *(Prikaz 6).*



Prikaz 6: Empirijske distribucije prosječnog vremena između transakcija za legitimne i prevarantske račune

Učestalost slanja transakcija pokazuje se kao vrijedan indikator potencijalno sumnjivog ponašanja. Iako sama po sebi možda nije dovoljno snažna za donošenje konačnog zaključka o prevari, u kombinaciji s drugim varijablama može značajno doprinijeti točnosti modela detekcije.

2.4 Jesu li računi koji šalju puno transakcija male vrijednosti češće sumnjivi?

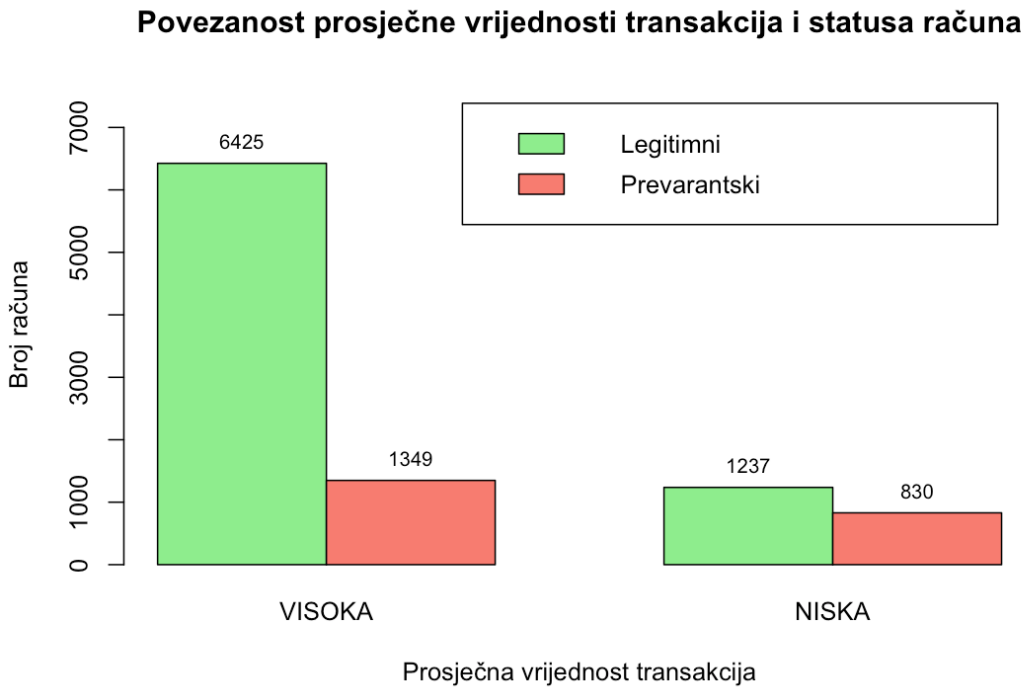
Ovaj dio istraživanja se temelji na prosječnoj vrijednosti poslanih transakcija po računu, budući da prevarantski računi često šalju velik broj transakcija s vrlo malim iznosima, strategijom poznatom kao *dusting attacks* ili *airdrop spam.*

Za usporedbu distribucija između legitimnih i prevarantskih računa korišten je *Mann–Whitney–Wilcoxon* test (*MWW*), neparametarski test koji pokazuje razliku u distribucijama između dviju skupina. Rezultati pokazuju p-vrijednost manju od 0.05, što potvrđuje statistički značajnu razliku u prosječnim vrijednostima transakcija između legitimnih i prevarantskih računa. Računi su razvrstani u dvije skupine: one s niskom prosječnom vrijednošću transakcija i one s normalnom ili visokom prosječnom vrijednošću. Prema *Tablici 3,* oko 40% računa s niskim iznosima povezano je s prevarama, dok je udio prevara u skupini s višom prosječnom vrijednošću samo 17%.

Low_Avg_Val_Sent	FLAG = 0 (Legitimno)	FLAG = 1 (Prevara)
FALSE (nije niska vrijednost)	82,65	17,35
TRUE (niska vrijednost)	59,85	40,15

Tablica 3: Omjer prevarantskih i legitimnih računa prema aktivnosti u broju poslanih transakcija

Prikaz 7 vizualno ilustrira razliku u udjelu legitimnih i prevarantskih računa između ovih skupina.



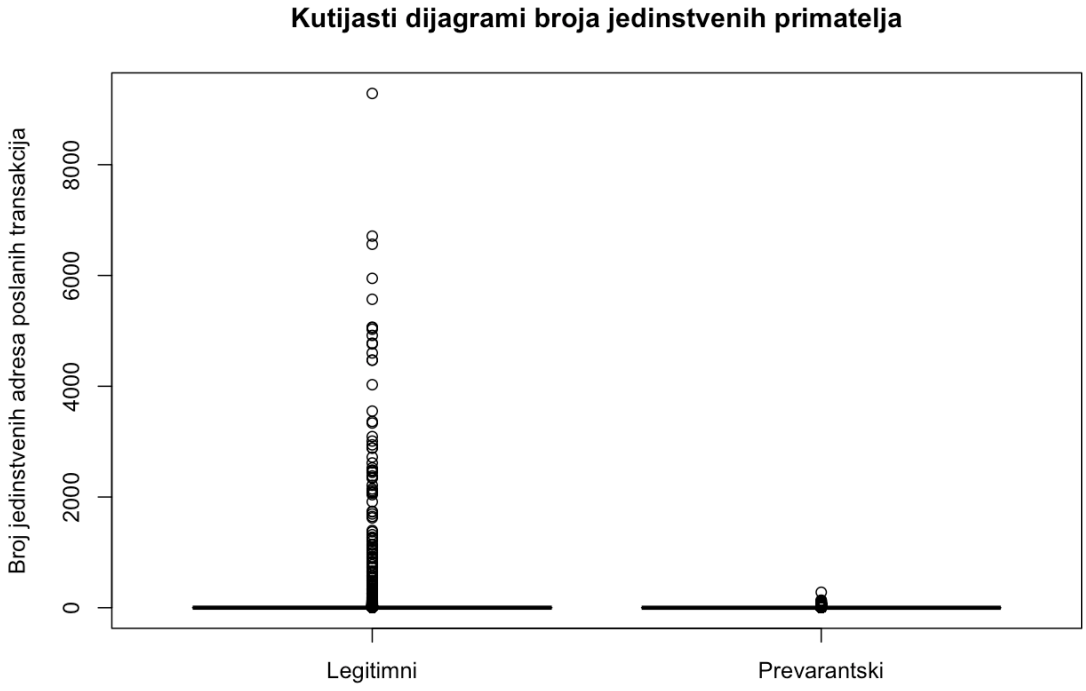
Prikaz 7: Stupčasti dijagrami računa s niskom i visokom prosječnom vrijednošću transakcija

Rezultati potvrđuju da transakcije male vrijednosti mogu biti snažan indikator sumnjivog ponašanja te predstavljaju vrijedan signal u kombinaciji s drugim varijablama pri izgradnji modela detekcije prevara.

2.5 Analiza broja jedinstvenih adresa kojima računi šalju transakcije

Jedan od pokazatelja razlikovanja legitimnih i prevarantskih računa je broj jedinstvenih adresa kojima se šalju transakcije. Ova varijabla odražava širinu mreže primatelja i može otkriti obrasce ponašanja karakteristične za određeni tip računa.

Prikaz 8 pokazuje da legitimni računi češće komuniciraju s većim brojem različitih adresa, dok prevarantski računi šalju transakcije ograničenom broju primatelja, što upućuje na ciljan i zatvoren način djelovanja.



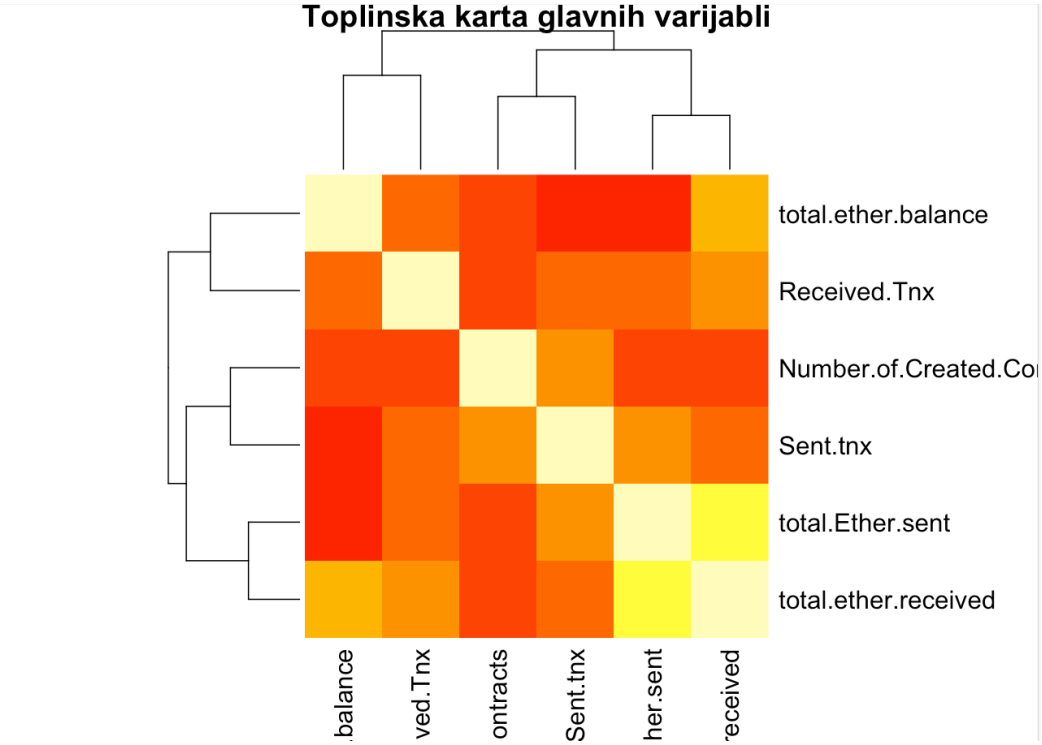
Prikaz 8: Kutijasti dijagrami usporedbe broja jedinstvenih primatelja za legitimne i prevarantske račune: legitimni računi komuniciraju šire od prevarantskih

Za statističku potvrdu razlika korišten je *Wilcoxonov U test (Mann–Whitney–Wilcoxon)*, neparametarski test koji ne pretpostavlja normalnost distribucije. Test je pokazao p-vrijednost manju od 2.2e-16, što znači da odbacujemo nultu hipotezu i potvrđujemo statistički značajnu razliku između legitimnih i prevarantskih računa u broju jedinstvenih adresa kojima šalju transakcije.

Ova analiza naglašava važnost promatranja distribucije transakcijskih partnera kao potencijalnog indikatora sumnjivog ponašanja na blockchain mrežama.

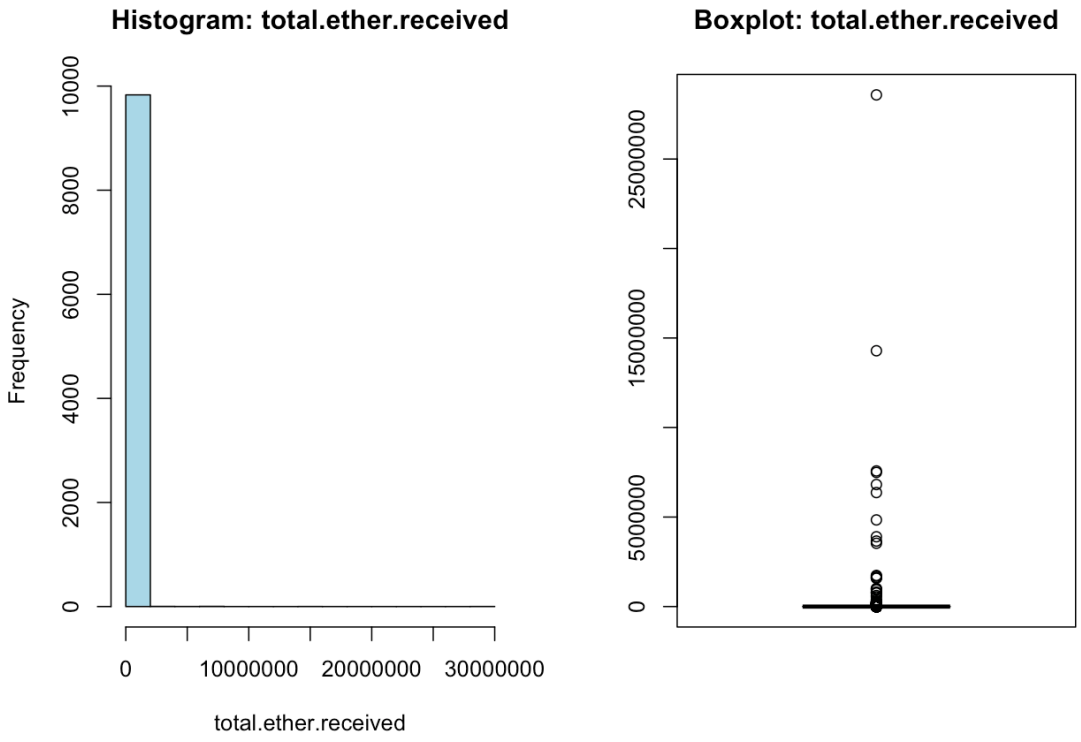
2.6 Analiza veza među varijablama temeljena na Spearmanovom koeficijentu korelacije

Za dublje razumijevanje međusobnih odnosa između varijabli koje odražavaju transakcijsko ponašanje adresa na Ethereum mreži, provedena je analiza usmjerena na postojanje monotonih veza među varijablama: *total.ether.received*, *total.Ether.sent* i *total.ether.balance*. Analiza je prethodno bila motivirana rezultatima prikazanim u korelacijskoj matrici (*Prikaz 9*), gdje su identificirani odnosi različitog intenziteta među tim varijablama.



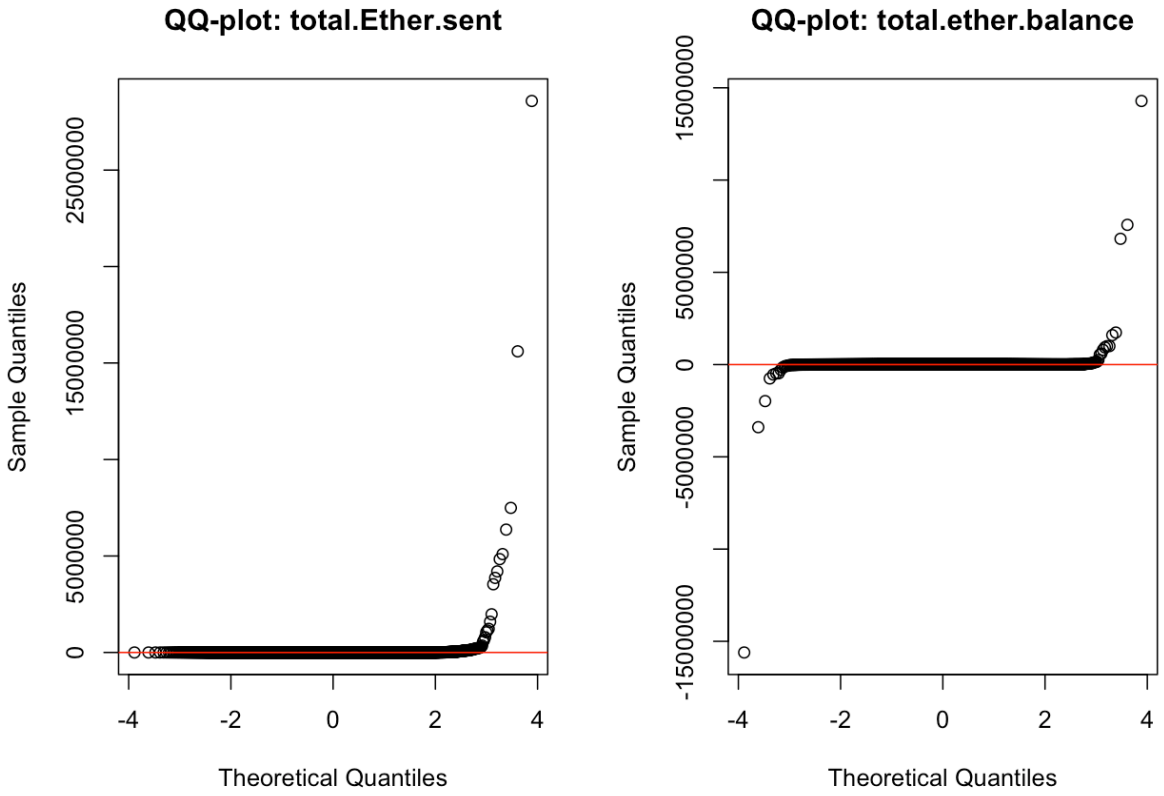
Prikaz 9: Toplinska karta glavnih varijabli

Prije provođenja testova o odstutnosti monotonih veza, izvršena je procjena distribucija ključnih varijabli radi odabira prikladnog statističkog testa. Histogram i kutijasti dijagram varijable *total.ether.received (Prikaz 10)* jasno pokazuju visoku asimetriju - većina vrijednosti je koncentrirana vrlo blizu nule, dok su stršeće vrijednosti ekstremno velike.



Prikaz 10: Histogram i kutijasti dijagram varijable total.ether.received s naglašenom asimetrijom

Iste rezultate dobivamo za varijable *total.Ether.sent* i *total.ether.balance*, što je prikazano Q-Q dijagramima (*Prikaz 11).*



Prikaz 11: Q-Q dijagrami za procjenu normalnosti distribucije ukupno poslanog Ethera i stanja računa

Stoga, kako bi se izbjegao utjecaj outliera i kršenje pretpostavki o normalnosti, umjesto Pearsonove korelacije primijenjena je Spearmanova rang korelacija, koja je adekvatnija u ovakvim uvjetima.

2.6.1 *total.ether.received* vs *total.Ether.sent*

Spearmanov test o postojanju monotone veze ($\rho \approx 0.775$) daje p < 2.2e-16. Možemo zaključiti da među varijablama postoji snažna pozitivna monotona povezanost, što znači da njihovu vezu ima smisla modelirati nekom monotono rastućom funkcijom (tj. adrese koje primaju više Ethera u pravilu šalju više). Budući da *Spearman* mjeri rangove, ova povezanost ne mora biti linearna, ali pokazuje stabilan smjer veze. Takva dinamika sugerira prisutnost čvorišta visoke aktivnosti, poput razmjena, mjenjačnica ili servisa koji imaju veliki promet u oba smjera.

2.6.2 *total.ether.received* vs *total.ether.balance*

Iako bi se intuitivno moglo smatrati vjerojatnim da će adrese koje prime velike količine Ethera imati i visoke saldo vrijednosti, Spearmanov test o postojanju monotone veze ($\rho \approx 0.357$) ukazuje na tek umjerenu monotono rastuću vezu (p < 2.2e-16). To znači da, iako postoji tendencija da veći unos Ethera prati i veći saldo, ta veza nije dosljedna ni jaka.

Spearmanov ρ ovdje procjenjuje u kojoj se mjeri redoslijedi (rangovi) vrijednosti dviju varijabli slažu. Umjerena razina povezanosti sugerira da adrese koje primaju više Ethera ne zadržavaju nužno veće količine - vjerojatno zato što mnoge od njih (poput burzi, pametnih ugovora ili aktivnih servisa) odmah redistribuiraju sredstva, što utječe na njihov krajnji saldo.

Vizualno, ova slabija monotona veza potvrđena je srednje intenzivnom žuto-narančastom nijansom u korelacijskoj heatmapi, što korespondira s nižim Spearmanovim koeficijentima u odnosu na druge parove varijabli.

2.6.3 *total.Ether.sent* vs *total.ether.balance*

Spearmanov koeficijent ukazuje na padajuću monotonu vezu ($\rho \approx$ -0.314, p < 2.2e-16). To znači da adrese koje šalju veće količine Ethera imaju tendenciju imati niži završni saldo. Iako asocijacija nije jaka, jasno je izražena negativna povezanost u redoslijedu vrijednosti. Adrese koje su više rangirane po količini poslanog Ethera najčešće su niže rangirane po preostalom balansu.

Ova veza ima logično objašnjenje: slanje većih količina Ethera smanjuje saldo, osobito kod adresa koje služe kao prijelazne točke (npr. adrese koje „ispuštaju“ sredstva prema drugim adresama). Takav obrazac ponašanja može ukazivati na automatizirane transakcije, centralizirane servise ili čak potencijalno sumnjive aktivnosti poput „pražnjenja“ računa.

Vizualno, ova padajuća monotona veza prikazana je tamnijom narančastom nijansom u korelacijskoj mapi, što je u skladu s negativnim predznakom Spearmanovog koeficijenta i slabijom povezanošću u rangovima.

2.6.4 Refleksija

Ispitivanje asocijacija između navedenih varijabli omogućilo je prepoznavanje obrazaca ponašanja korisnika na mreži. Jaka asocijacija između *total.ether.received* i *total.Ether.sent* sugerira postojanje adresa koje sudjeluju u velikom broju transakcija, često i kao posrednici ili razmjene. S druge strane, negativna monotona povezanost između *total.Ether.sent* i *total.ether.balance* može pomoći u otkrivanju adresa koje imaju operativnu funkciju - šalju sredstva, ali nemaju dugoročni saldo, što je česta pojava u aktivnostima poput pranja novca.

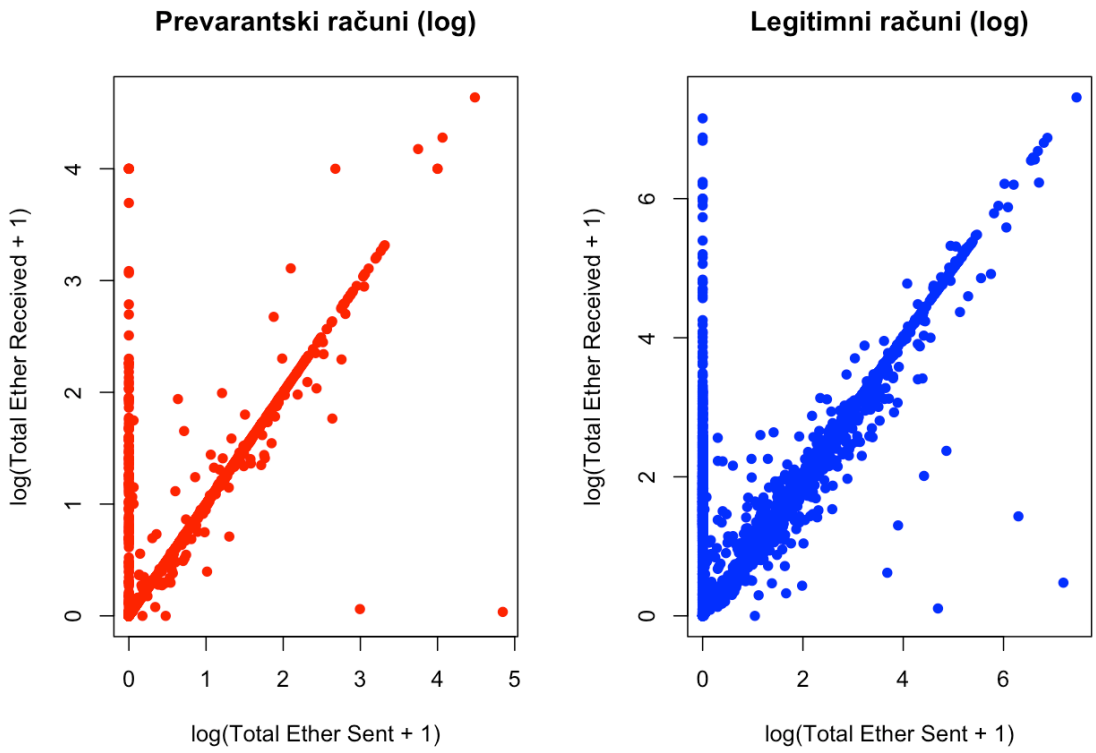
Odabrane varijable su analizirane zbog njihove temeljne uloge u financijskom prometu na blockchainu: *total.ether.received* i *total.Ether.sent* predstavljaju inpute i outpute, dok *total.ether.balance* odražava neto stanje. Njihovom usporedbom dobivamo sliku ne samo o količini, nego i o obrascima kretanja sredstava, što je ključno za daljnju klasifikaciju adresa i izgradnju prediktivnih modela u kontekstu sigurnosti, praćenja aktivnosti i otkrivanja anomalija.

2.7 Analiza odnosa ukupno poslanog i primljenog Ethera

U svrhu prepoznavanja obrazaca ponašanja između prevarantskih i legitimnih računa na Ethereum mreži, analizirane su varijable *Total Ether Sent* i *Total Ether Received*, koje predstavljaju ukupnu količinu Ethera koju je pojedini račun poslao, odnosno primio tijekom svog postojanja. Ove dvije varijable pružaju kvantitativni uvid u financijsku aktivnost računa, a osobito su korisne za razlikovanje tipičnih korisničkih ponašanja od potencijalno sumnjivih.

Kako bi se bolje prikazali podaci koji uključuju ekstremne vrijednosti (npr. računi s izuzetno velikim količinama Ethera), korištena je logaritamska transformacija podataka funkcijom $\log(x+1)$. Takva transformacija smanjuje utjecaj outliera i omogućuje precizniju vizualnu interpretaciju distribucije računa.

Na *Prikazu 12* vidimo dva dijagrama raspršenosti: s lijeve strane nalaze se prevarantski računi (označeni crvenom bojom), a s desne legitimni računi (označeni plavom bojom). Na x-osi je prikazana logaritamski transformirana vrijednost ukupno poslanog Ethera, dok je na y-osi ukupno primljeni Ether.



Prikaz 12: Dijagrami raspršenosti prema tipu računa

Kod legitimnih računa uočen je znatno širi raspon aktivnosti. Brojne točke nalaze se duž dijagonale grafa, što upućuje na uravnotežen omjer između primanja i slanja Ethera, što je i očekivano za račune koji sudjeluju u redovnim transakcijama, poput korisničkih novčanika ili razmjena.

Kako bi se vizualna opažanja dodatno potvrdila statistički, provedeni su neparametarski *MWW* testovi, s obzirom na to da podaci ne zadovoljavaju uvjete normalnosti distribucije.

Za varijablu *Total Ether Received*, testirane su sljedeće hipoteze:

H_0: Ne postoji razlika u distribucijama količine ukupno primljenog Ethera između prevarantskih i legitimnih računa.

H_1: Distribucija ukupno primljenog Ethera za prevarantske račune ima pozitivan lokacijski pomak u odnosu na distribuciju primljenog Ethera legitimnih računa.

Rezultati testa (p-vrijednost = 1) idu u prilog nul-hipotezi, pa ne možemo tvrditi da postoji razlika u distribucijama primljenog Ethera između prevarantskih i legitimnih računa.

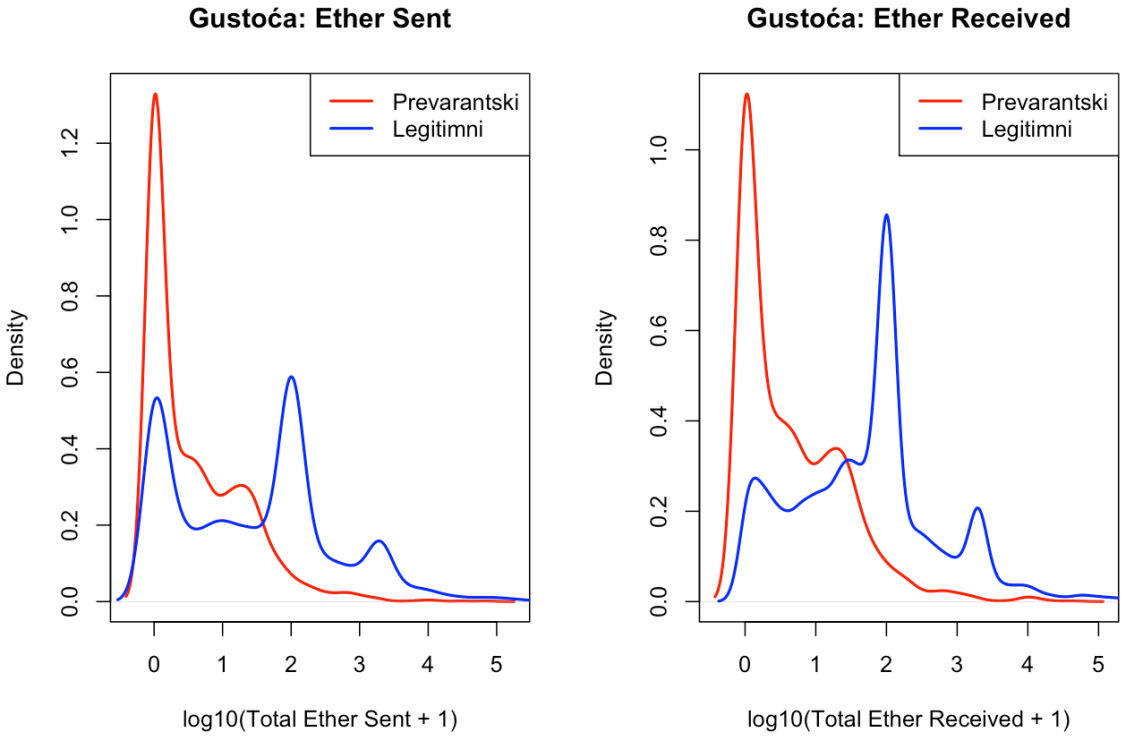
Za varijablu *Total Ether Sent*, testirane su hipoteze:

H_0: Ne postoji razlika u distribucijama količine ukupno poslanog Ethera između prevarantskih i legitimnih računa.

H_1: Distribucija ukupno poslanog Ethera za prevarantske račune ima pozitivan lokacijski pomak u odnosu na distribuciju primljenog Ethera legitimnih računa.

Ovaj test pokazao je izuzetno značajan rezultat (p-vrijednost $<$ 2.2e-16), što jasno potvrđuje alternativnu hipotezu: prevarantski računi šalju značajno manje Ethera. Ovo ponašanje je u skladu s očekivanjima jer takvi računi često služe kao krajnja odredišta sredstava, bez daljnjeg sudjelovanja u mrežnim transakcijama.

Radi dodatne potvrde razlika u distribucijama, napravljena je glatka procjena gustoće. Na *Prikazu 13* vidimo procjenjene gustoće distribucija za varijable *Total Ether Sent* i *Total Ether Received,* ponovno u log-skali. Crvena linija odnosi se na prevarantske, a plava na legitimne račune.



Prikaz 13: Gustoće distribucija za varijable Total Ether Sent i Total Ether Received

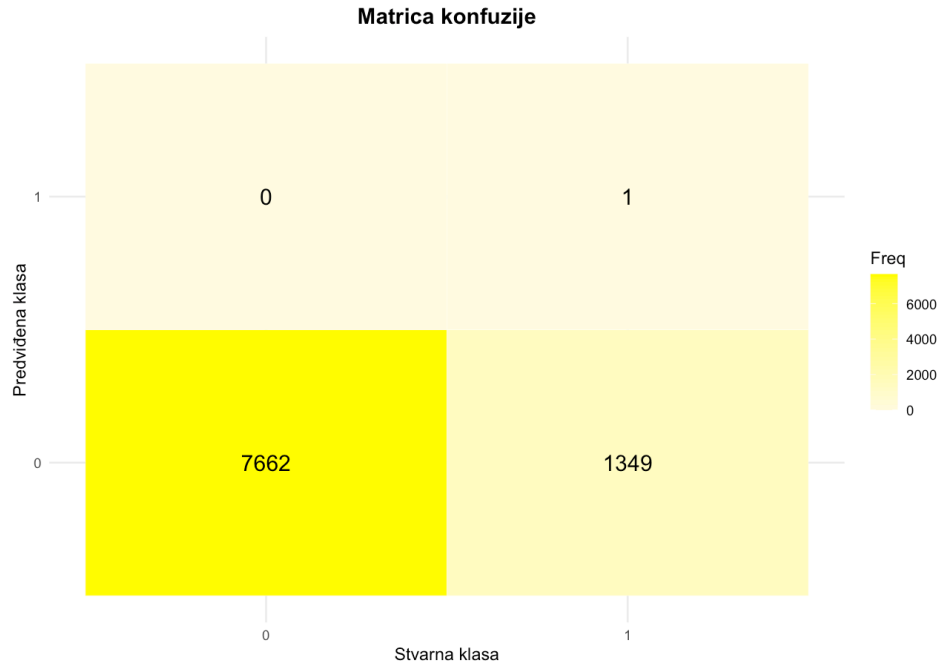
Jasno se vidi da je distribucija prevarantskih računa uža i pomaknuta prema nižim vrijednostima, osobito kada je riječ o poslanom Etheru. Legitimni računi pokrivaju širi raspon i imaju izraženiji "rep" distribucije, što ukazuje na postojanje računa s većim količinama prenesenog Ethera.

Zaključno, i vizualna analiza i statistički test ukazuju na jasne razlike između prevarantskih i legitimnih računa. Dok legitimni računi pokazuju uravnoteženu aktivnost slanja i primanja Ethera, prevarantske račune karakterizira nizak volumen slanja i ograničena ukupna aktivnost. Njihove aktivnosti su usmjerene na mali obujam transakcija, što može biti posljedica pokušaja prikrivanja aktivnosti ili testiranja mreže. Raspodjele su usko fokusirane, bez izraženih "repova" prema višim vrijednostima, što znači da prevarantski računi rijetko rukovode velikim količinama Ethera.

2.8.1 Izrada i analiza logističkog modela za klasifikaciju transakcija

U ovom dijelu rada izrađen je logistički regresijski model s ciljem predviđanja vjerojatnosti da je transakcija označena kao sumnjiva ili prevarna (varijabla $FLAG$). Model je građen koristeći skup varijabli koje opisuju karakteristike transakcija, uključujući ukupne količine poslanog i primljenog Ethera, broj jedinstvenih adresa s kojima je transakcija komunicirala, broj kreiranih ugovora, prosječne vrijednosti poslanih i primljenih transakcija, te relevantne ERC20 token varijable.

Nakon fitanja modela na dostupnim podacima, izračunate su predviđene vjerojatnosti pripadnosti klasi sumnjivih transakcija ($FLAG = 1$). Predikcije su zatim binarizirane pomoću praga 0.5 kako bi se dobile konačne klasifikacije i izračunala točnost modela. Dobivena točnost modela iznosila je približno 85.03%.



Prikaz 14: Matrica konfuzije logističkog regresijskog modela

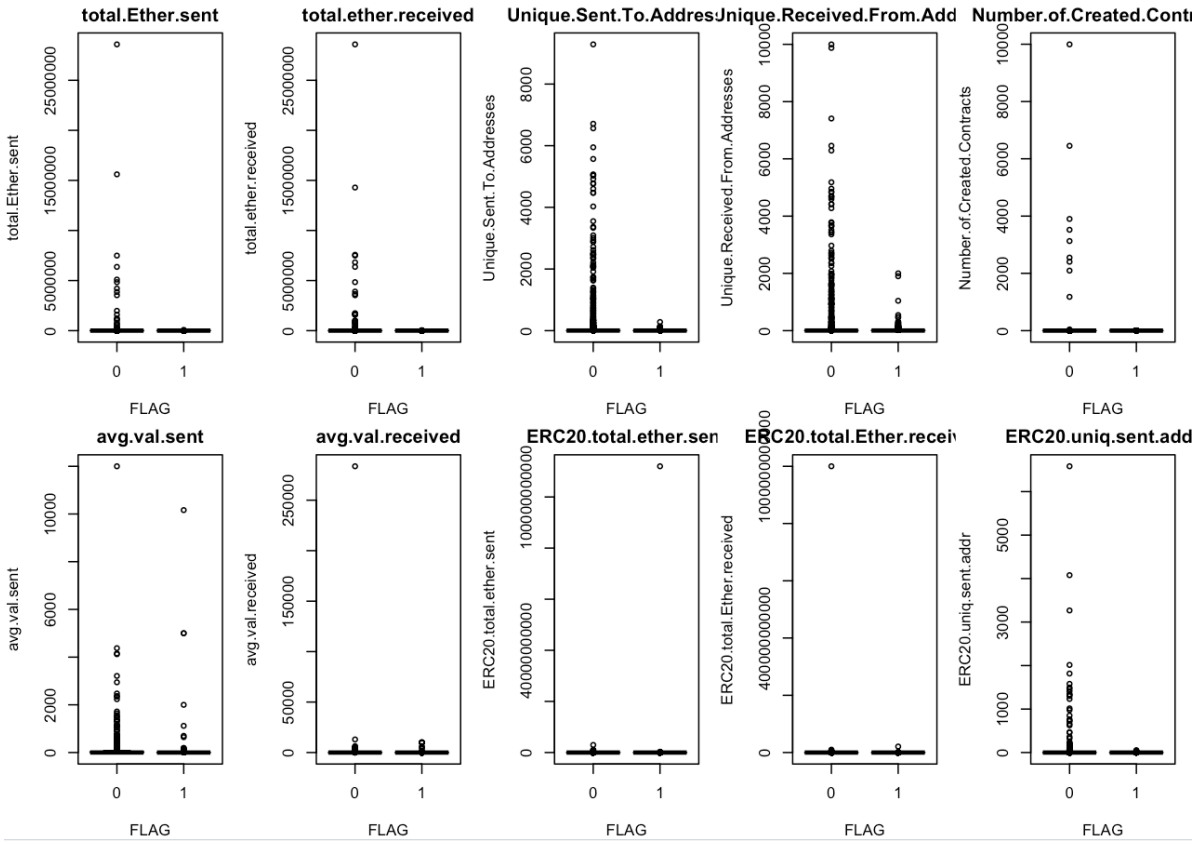
Važno je ukazati na neravnotežu među klasama u podacima, što se može uočiti u tablici proporcija.

FLAG	Udio
0	77,86
1	22,14

Tablica 4: Tablica proporcija udjela pojedinog tipa računa

Legitimne transakcije ($FLAG = 0$) čine 77.86% skupa, dok je udio sumnjivih ili prevarnih transakcija ($FLAG = 1$) značajno manji, 22.14%. Ova neravnoteža utječe na model tako da on "igra na sigurno" i favorizira većinsku klasu, nastojeći maksimizirati ukupnu točnost.

Dodatno, iz kutijastih dijagrama varijabli po klasama vidi se da su distribucije prediktora vrlo slične za obje klase. To znači da model nema jasne značajke koje bi razlikovale legitimne i sumnjive transakcije, pa je njegova sposobnost razlikovanja ograničena. Zbog toga model generira niske predviđene vjerojatnosti za klasu sumnjivih transakcija, pa čak i kod stvarno sumnjivih transakcija predikcije ostaju blizu nule.



Prikaz 15: Kutijasti dijagrami glavnih transakcijskih varijabli prema statusu računa

2.8.2 Interpretacija rezultata

Predikcije su dobivene izračunom vjerojatnosti da račun pripada klasi $FLAG = 1$ pomoću modela logističke regresije. Vjerojatnosti veće od 0.5 pretvorene su u predviđene klase 1, a ostale u klase 0. Točnost modela izračunata je kao udio ispravno klasificiranih opažanja u odnosu na ukupni broj opažanja te iznosi 85.03 %.

Iako je model postigao ukupnu točnost od oko 85%, detaljna analiza pokazuje da model gotovo sve transakcije klasificira kao sigurne ($FLAG = 0$). Ovaj rezultat proizlazi iz:

- Neravnoteže klasa, gdje većina transakcija (76.6%) pripada klasi sigurnih (*Tablica 5*)
- Sličnosti distribucija značajki između sigurnih i sumnjivih transakcija (*Prikaz 19*)
- Slabe razlikovne moći odabranih varijabli

Model se stoga može interpretirati kao da je "naučio" predviđati većinsku klasu, a ne uspijeva u potpunosti ispravno prepoznati sumnjive transakcije.

Međutim, podatak da je točnost modela oko 85% (dok je udio legitimnih transakcija 78%), ipak nam govori da je model uspješno prepoznao pojedine lažne transakcije.

Ovaj nalaz naglašava važnost pažljivog pristupa kod problema s neravnoteženim podacima i potrebu za dodatnim metodama obrade podataka (npr. balansiranje klasa, složeniji modeli ili dodatne značajke) za učinkovitiju detekciju prevara.

3 Primjena Benfordovog zakona za detekciju sumnjivih transakcija

Ovdje je predstavljen prijedlog metodologije za automatiziranu detekciju sumnjivih transakcija na Ethereum mreži, koji se temelji na Benfordovom zakonu. Radi se o distribuciji vodećih znamenki koja se prirodno javlja u brojnim numeričkim skupovima podataka, osobito onima koji obuhvaćaju više redova veličine - kao što su financijske transakcije, demografski podaci, cijene ili računi.

Vodeća znamenka realnog broja x (pri čemu $x > 0$) definirana je kao prva nenulta znamenka u njegovom zapisu, odnosno kao cijeli broj $d \in 1, \ldots, 9$ takav da vrijedi: $d = \lfloor 10 \lfloor \log_x \rfloor x \rfloor$. Ova definicija proizlazi iz znanstvene notacije broja $x = d \cdot 10^k$, gdje je $1 \leq d < 10$, a d je tada vodeća znamenka.

Prema Benfordovom zakonu će se znamenka 1 pojaviti kao vodeća u oko 30% slučajeva, dok će znamenka 9 biti vodeća znatno rjeđe – u oko 4.6% slučajeva. Benfordova distribucija definira se sljedećom logaritamskom funkcijom:

$P(d) = \log\left(1 + \frac{1}{d}\right), \quad d = 1, \ldots, 9.$

Odstupanja od ove distribucije mogu ukazivati na nepravilnosti, automatizirano ponašanje, manipulirane podatke ili prikrivene obrasce – zbog čega se Benfordov zakon već godinama koristi u financijskoj forenzici, primjerice u otkrivanju poreznih prevara, revizijama poduzeća ili analizama *Ponzi shema*.

3.1 Metodološki okvir

Cilj ovog dijela projekta je razviti sustav koji automatizira:

- ekstrakciju vodeće znamenke iz različitih kvantitativnih varijabli
- usporedbu njihove empirijske distribucije s teorijskom Benfordovom distribucijom
- kvantifikaciju odstupanja pomoću statističkih mjera (χ^2 test, srednje apsolutno odstupanje - MAD)
- identifikaciju onih računa ili skupina transakcija čije ponašanje značajno odstupa od predviđenog uzorka

Na taj način moguće je detektirati transakcije koje možemo okarakterizirati kao sumnjive, odnosno kao kandidate za dublju inspekciju.

3.2 Benfordova analiza varijable *total.Ether.sent*

Kao početni korak u testiranju predložene metodologije, Benfordov zakon primijenjen je na numeričku varijablu *total.Ether.sent*, koja predstavlja ukupnu količinu Ethera koju je pojedini račun poslao. Ova varijabla obuhvaća širok raspon vrijednosti – od mikrotransakcija do milijunskih iznosa – što je čini iznimno prikladnom za ovakvu vrstu analize.

Cilj analize bio je ispitati postoji li odstupanje u distribuciji vodećih znamenki koje bi moglo ukazivati na:

- neprirodno generirane vrijednosti
- koordinirane obrasce ponašanja
- prisutnost botova ili skrivenih strategija na mreži

Kao ilustracija predloženog pristupa, Benfordov zakon primijenjen je na varijablu *total.Ether.sent*, koja označava ukupnu količinu Ethera poslanog s pojedinog računa. Ova varijabla bila je posebno zanimljiva jer pokriva širok spektar vrijednosti – od vrlo malih transakcija do iznosa koji prelaze više milijuna jedinica, čime zadovoljava osnovni preduvjet za Benfordovu analizu: prisutnost podataka kroz više redova veličine.

Primarni cilj bio je ispitati postoje li odstupanja u distribuciji vodeće znamenke u odnosu na teorijsku pretpostavku. Pretpostavka je da bi značajna odstupanja mogla ukazivati na nepravilnosti – primjerice, generirane ili ponavljajuće vrijednosti, što je česta praksa kod automatiziranih (bot) računa ili računa uključenih u sumnjive aktivnosti.

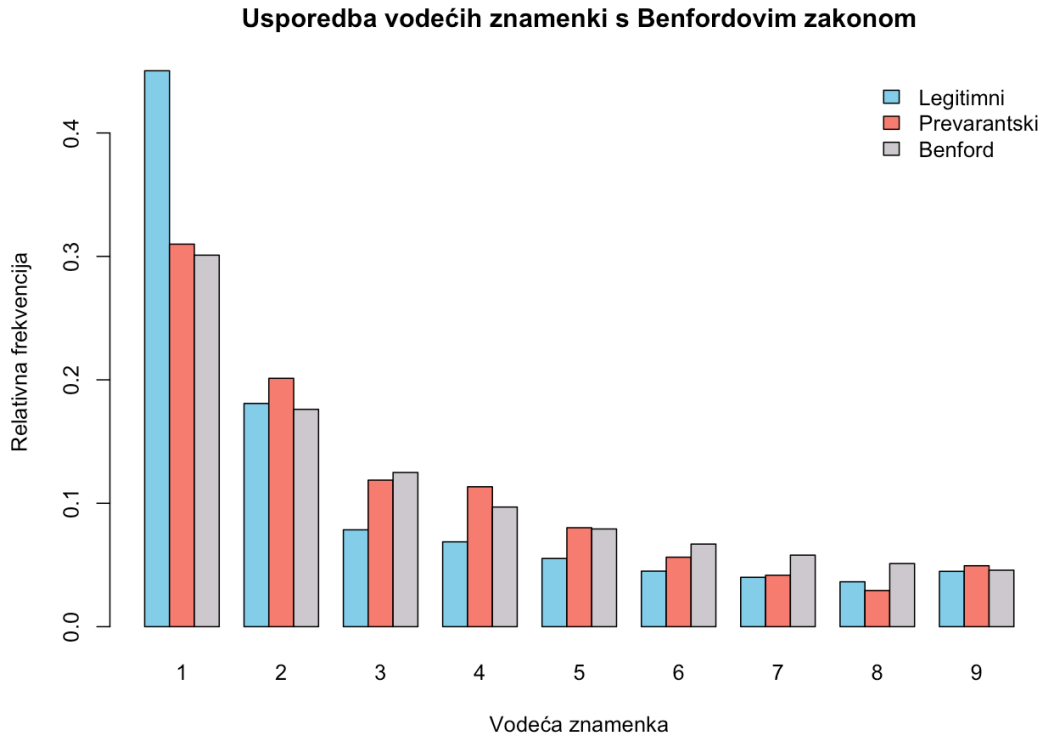
Za zaključivanje primijenjena su dva pristupa:

- χ^2 test podudarnosti, kojim se statistički procjenjuje razlikuje li se empirijska distribucija vodećih znamenki od predviđene (teorijske) prema Benfordovu zakonu
- srednje apsolutno odstupanje (MAD), kao nenadzirana mjera prosječne razlike između stvarne i teorijske distribucije

Analiza je provedena odvojeno za legitimne i za prevarantske račune, kako bi se uočile potencijalne razlike u obrascima ponašanja. Zanimljivo je da su legitimni računi pokazivali značajnija odstupanja u odnosu na Benfordovu distribuciju (χ^2 p-vrijednost ≈ 0.0001, MAD ≈ 0.037), dok su prevarantski računi bili bliže teorijskoj raspodjeli (p ≈ 0.4, MAD ≈ 0.013).

Ovi rezultati mogu djelovati kontraintuitivno – legitimni računi pokazuju odstupanja, dok se prevarantski čine "urednijima". No, upravo takvi nalazi mogu ukazivati na sofisticiranost prevara: zlonamjerni akteri mogu namjerno oblikovati transakcijske uzorke kako bi oponašali prirodnu distribuciju i time izbjegli detekciju.

Vizualna usporedba raspodjele vodećih znamenki dodatno potvrđuje ove razlike. Na prikazanom grafikonu jasno se vidi veće odstupanje empirijske distribucije vezane uz legitimne račune od Benfordove distribucije, dok distribucija prevarantskih računa znatno bolje prati Benfordovu distribuciju – osobito kod znamenki 1, 3 i 4.



Prikaz 16: Distribucija vodećih znamenki kod različitih tipova računa za varijablu total.Ether.sent

3.3 Benfordova analiza varijable *total.ether.balance*

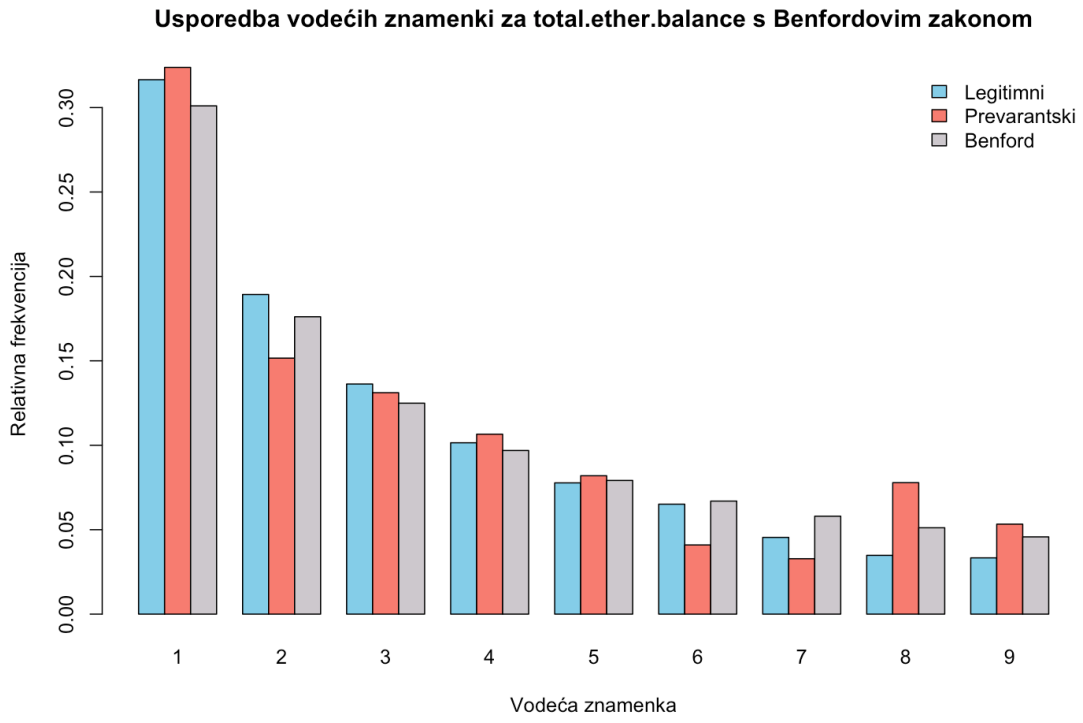
U nastavku analize primijenjen je Benfordov zakon na numeričku varijablu *total.ether.balance*, koja označava ukupnu količinu Ethera prisutnu na pojedinom računu u trenutku analize. Ova varijabla sadrži vrijednosti koje obuhvaćaju širok raspon – od računa s minimalnim iznosima do onih s milijunskim balansima – čime također zadovoljava osnovni preduvjet za primjenu Benfordove distribucije: prisutnost višestrukih redova veličine.

Analiza je ponovno provedena za dvije odvojene skupine – legitimne i prevarantske račune – kako bi se utvrdile moguće razlike u obrascima.

Za procjenu odstupanja korišteni su isti pristupi:

- χ^2 test podudarnosti, za statističko ispitivanje razlike između empirijske i teorijske distribucije vodećih znamenki
- Srednje apsolutno odstupanje (MAD), koje mjeri prosječnu razliku između promatranih i predviđenih frekvencija

Rezultati analize usklađenosti distribucije varijable *total.ether.balance* s Benfordovom distribucijom pokazuju zanimljiv obrazac: distribucija vodećih znamenki legitimnih računa značajno odstupa od predviđene (χ^2 p-vrijednost ≈ 0.00038; MAD ≈ 0.020), uz precjenjivanje znamenki 1 i 2 te podzastupljenost znamenki 6–9. Suprotno tome, distribucija vodećih znamenki prevarantskih računa bolje je usklađena s teorijskom Benfordovom distribucijom (χ^2 p-vrijednost ≈ 0.24; MAD ≈ 0.012). Ovi rezultati sugeriraju da su prevarantski računi često sofisticirani i prilagođeni kako bi izgledali „prirodno“, dok legitimni računi odražavaju stvarnu tržišnu dinamiku, što ih čini podložnijima odstupanjima od idealne matematičke distribucije.



Prikaz 17: Distribucija vodećih znamenki kod različitih tipova računa za varijablu total.ether.balance

Vizualna analiza dodatno potvrđuje ove nalaze – empirijske frekvencije vodećih znamenki prevarantskih računa bolje prate teorijske vrijednosti prema Benfordovoj distribuciji, dok legitimni računi pokazuju odstupanja, osobito kod znamenki 1, 6 i 8.

3.4 Benfordova analiza varijable *avg.val.recieved*

Analiza distribucije vodećih znamenki provedena je i za varijablu *avg.val.received*, koja predstavlja prosječan iznos Ethera primljen po transakciji. Iako ova varijabla pokriva širok raspon vrijednosti, rezultati ponovno pokazuju slabu usklađenost distribucije varijable s Benfordovom distribucijom kod obje skupine.

Za legitimne račune, empirijska distribucija vodećih znamenki značajno odstupa od teorijske ($\chi^2 \approx 881.16$, $p < 2.2\text{e-}16$), pri čemu je posebno izražena prenaglašenost znamenke 1 ($\approx 39\%$) i 5 ($\approx 15\%$) te podcijenjenost znamenki 3, 4 i 6–9.

Slično tome, i kod prevarantskih računa dobiven je vrlo visoki χ^2 statistički pokazatelj (≈ 106.05, $p < 2.2\text{e-}16$), što također upućuje na znatna odstupanja, iako nešto blaža nego kod legitimnih računa.

U ovom slučaju, za razliku od prethodnih varijabli, obje skupine pokazuju nepodudarnost s Benfordovim zakonom, što može ukazivati na to da su mehanizmi određivanja prosječnih primljenih iznosa specifični i strukturirani, neovisno o legitimnosti računa – primjerice, zbog korištenja istih servisa, pametnih ugovora ili učestalih malih uplata.

3.5 Potencijalni razlozi odstupanja i daljnji smjer analize

Odstupanja od Benfordove distribucije primijećena kod više varijabli mogu imati različite uzroke. Jedan od ključnih faktora jest prisutnost velikog broja automatiziranih (bot) transakcija koje generiraju konzistentne, često zaokružene vrijednosti – osobito kod računa dizajniranih za masovno slanje ili primanje sredstava. Takvi računi narušavaju predviđenu distribuciju vodećih znamenki karakterističnu za podatke koji nastaju prirodnim, nenamjernim procesima.

Uz to, tehnička ograničenja mreže (npr. minimalna količina Ethera potrebna za izvršenje transakcije), ponavljajući uzorci korištenja pametnih ugovora, ili određene strategije korisnika (npr. zaobilaženje troškova plina) mogu dodatno utjecati na raspodjelu podataka, čime dolazi do sistematskih odstupanja – čak i kod legitimnih aktivnosti.

S obzirom na ove okolnosti, postavlja se pitanje je li razina transakcije najprikladniji sloj za ovu vrstu analize.

U daljnjoj fazi istraživanja, fokus će biti preusmjeren na agregirane vrijednosti, poput zbroja poslanih ili primljenih sredstava po danu, satu ili adresi. Takva agregacija može ublažiti utjecaj pojedinačnih anomalija i omogućiti jasniju identifikaciju obrazaca koji doista odražavaju transakcijske aktivnosti na mreži.

3.6 Primjena Benfordovog zakona na skup podataka o transakcijama s vremenskim oznakama

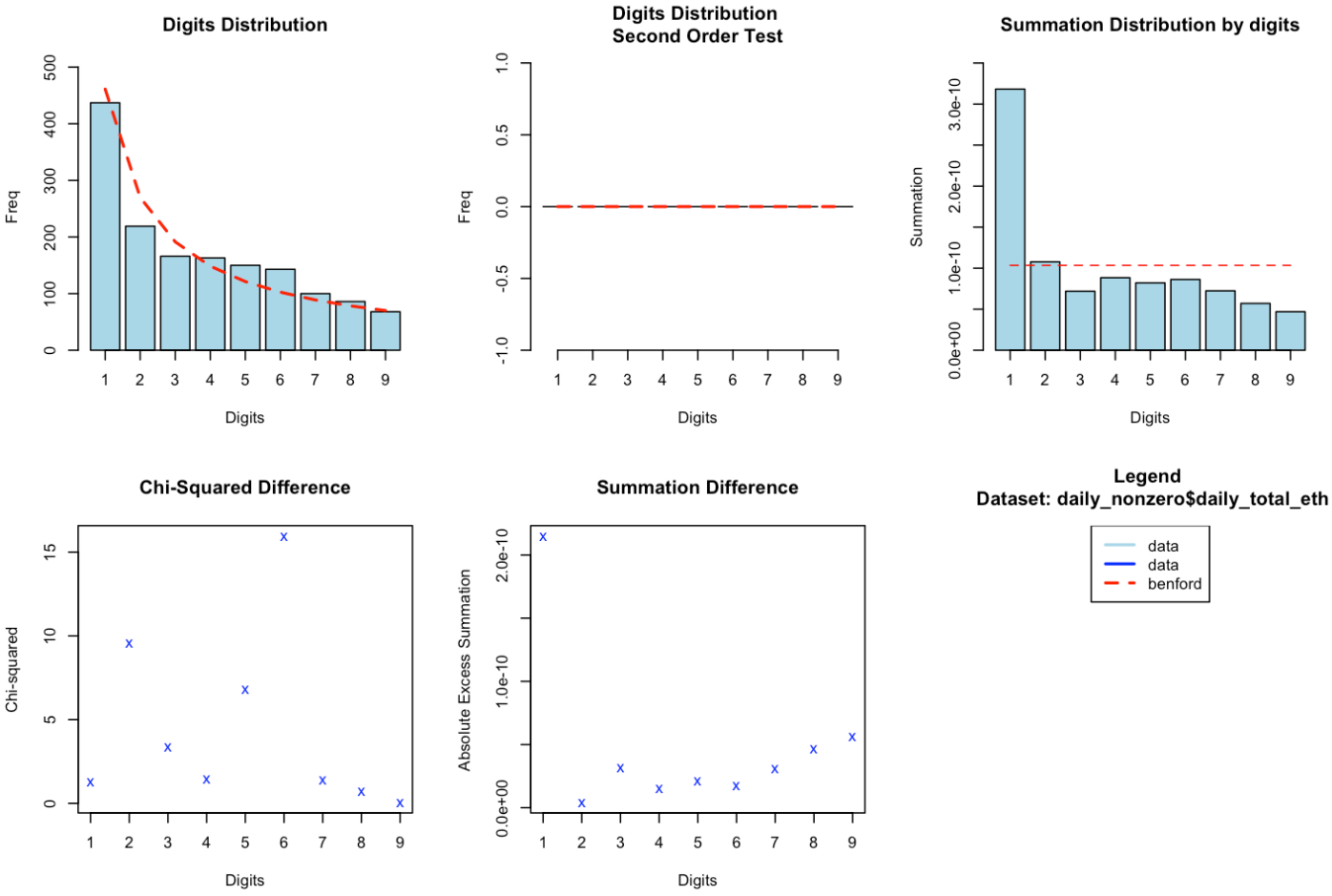
U analizu je uključen novi skup podataka koji, osim osnovnih podataka o transakcijama, sadrži i vremenske oznake, što je omogućilo agregaciju podataka prema vremenskim intervalima i detaljniji uvid u distribuciju vodećih znamenki. Korišteni skup podataka sadrži više od 6.7 milijuna transakcija na Ethereum mreži. Uz podatke o adresama, iznosima i vremenskim oznakama, ovaj skup uključuje i oznaku je li transakcija bila uspješna (*isError*), što je omogućilo filtriranje samo valjanih zapisa. Korišteni paket *benford.analysis* u R provodi statističke testove te izračunava mjere odstupanja poput prosječnog apsolutnog odstupanja *(MAD)* i *Z-score*, kako bi se ocijenilo koliko podaci prate Benfordov zakon.

Transakcijske vrijednosti izražene su u jedinici *Wei*, stoga je provedena konverzija u Ether kako bi rezultati bili interpretabilniji. Nakon toga, vremenske oznake transakcija pretvorene su u standardni kalendarski format i ukupna vrijednost svih transakcija grupirana je po danima.

Takva agregacija po datumu omogućila je analizu obrasca vodećih znamenki u dnevnoj ukupnoj vrijednosti transakcija. Time se uklanja "šum" koji proizlazi iz pojedinačnih, često automatiziranih transakcija s umjetno generiranim vrijednostima.

Na dobivenom nizu dnevnih zbrojeva primijenjena je Benfordova analiza. Rezultat analize pokazao je vrijednost MAD = 0.0149, što se prema standardima tumači kao "marginalno prihvatljivo odstupanje" od Benfordove distribucije.

Ovaj rezultat ukazuje na to da se vodeće znamenke u dnevno agregiranim vrijednostima u velikoj mjeri ponašaju u skladu s Benfordovim zakonom, što nije bio slučaj kod analize sirovih transakcija. Takav ishod podupire tezu da agregirani podaci bolje reflektiraju prirodne obrasce ponašanja te su pogodniji za statističke metode otkrivanja anomalija.



Prikaz 18: Rezultati Benfordove analize dnevno agregiranih ETH transakcija iz second_order_df

1. graf (s lijeva na desno) - Digits Distribution (Histogram učestalosti prve znamenke (1–9) u dnevnim sumama ETH):

Stvarna raspodjela prilično dobro prati Benfordov zakon - znak da podaci nisu manipulirani i ponašaju se prirodno.

2. graf - Digits Distribution – Second Order Test (Prikazuje razliku između stvarne distribucije i Benfordove po znamenkama):

Sve je na nuli, što znači da je odstupanje vrlo malo.

3. graf - Summation Distribution by Digits (Koliko ukupno svaka znamenka "vrijedi" - zbroj svih dnevnih iznosa koji počinju s tom znamenkom):

Značajna dominacija znamenke 1 - što je u skladu s Benfordovim zakonom.

4. graf - χ^2 Difference (Prikazuje vrijednosti χ^2 testa po znamenkama - veća vrijednost znači veće odstupanje od predviđene frekvencije):

Uočljivo je jedno veće odstupanje kod znamenke 6 - moguće nasumično ili uzrokovano određenim danima s velikim iznosima.

5. graf - Summation Difference (Apsolutna razlika između stvarnog i predviđenog zbroja po znamenkama):

Veća odstupanja su vidljiva kod znamenki 1 i 9, ali i dalje u prihvatljivim granicama.

U grafičkim prikazima rezultata Benfordove analize nad dnevno agregiranim vrijednostima ETH transakcija uočava se da stvarna distribucija prve znamenke u velikoj mjeri prati Benfordovu raspodjelu. Najčešća vodeća znamenka je 1, što je u skladu s teorijskim predviđanjima. Manja odstupanja vidljiva su kod znamenki 5 i 9, koje su blago precijenjene u odnosu na predviđenu frekvenciju, no ta odstupanja nisu statistički značajna. χ^2 test i grafovi potvrđuju da razlike između empirijskih i teorijskih vrijednosti ostaju u granicama prihvatljivog, dok vrijednost MAD = 0.0149 ukazuje na marginalno odstupanje.

Iako pojedinačne transakcije mogu pokazivati odstupanja od Benfordove distribucije zbog malih iznosa, zaobilaženja okrugljenja ili specifičnih obrazaca ponašanja korisnika, agregirane vrijednosti bolje prate Benfordov zakon. To se događa jer se prilikom agregacije nepravilnosti poput fiksnih iznosa, automatiziranih transakcija i lokalnih anomalija međusobno kompenziraju i razrjeđuju unutar većih skupova podataka. Na primjer, ponavljajuće vrijednosti koje proizlaze iz automatiziranih isplata ili naknada gube utjecaj kada se transakcije zbrajaju po vremenskim intervalima, čime ukupni iznosi bolje reflektiraju prirodnu raspodjelu transakcija. Na taj način agregirani podaci smanjuju utjecaj neprirodnih obrazaca i služe kao pouzdaniji indikator prirodnog i nekontroliranog ponašanja transakcija.

3.7 Analiza poznatih adresa: legitimne i prevarne aktivnosti

U prethodnim poglavljima analizirane su agregirane i sirove vrijednosti transakcija s Ethereum mreže, pri čemu su primijećena određena odstupanja od Benfordove distribucije. Međutim, takva analiza ostaje na općenitoj razini i ne omogućuje precizno razlikovanje između legitimnih i potencijalno sumnjivih aktivnosti. Kako bi se detaljnije sagledali obrasci ponašanja, ova faza istraživanja usmjerena je na analizu pojedinačnih Ethereum adresa koje su prethodno klasificirane kao legitimne (npr. poznate javne osobe ili institucije) ili prevarne (npr. označene na blockchainu kao povezane s prevarama, *phishingom* ili *rug pullovima*).

Korištenjem Benfordove analize nad transakcijskim podacima takvih adresa moguće je ispitati u kojoj mjeri njihovo ponašanje odstupa od predviđene distribucije vodećih znamenki – te je li to odstupanje dovoljno konzistentno da posluži kao signal za detekciju nepravilnosti.

3.7.1 Vitalik Buterin – poznata legitimna adresa

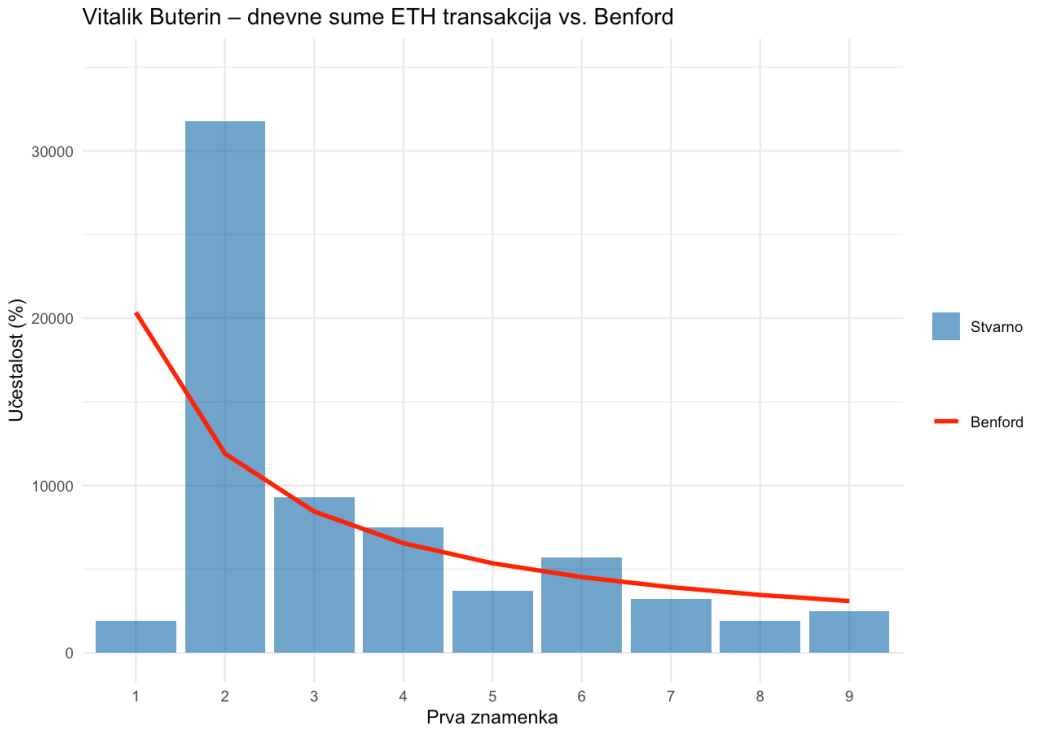
U ovoj analizi korišteni su transakcijski podaci za adresu Vitalika Buterina, suosnivača Ethereuma, s vremenskim rasponom aktivnosti od 2015. do 2025. godine. Budući da je riječ o visoko poznatoj i legitimnoj adresi, očekuje se da su njezine transakcije uglavnom netržišne i pod visokom kontrolom.

Postupak analize uključivao je sljedeće korake:

- Učitavanje podataka iz CSV datoteke koja sadrži detaljne informacije o vrijednosti transakcija u razdoblju 2015.-2025. godine
- Izračun ukupne dnevne aktivnosti u ETH zbrajanjem ulaznih i izlaznih vrijednosti *(Value_IN(ETH) + Value_OUT(ETH))*
- Pretvorba *UNIX* vremenskih oznaka u čitljive datume, što omogućuje grupiranje transakcija po danima
- Filtriranje samo onih dana kada je došlo do prijenosa sredstava, čime se isključuju transakcije bez financijske vrijednosti
- Agregacija dnevnih vrijednosti, odnosno sumiranje ukupne ETH aktivnosti po svakom danu
- Primjena Benfordove analize na prve znamenke dnevnih suma, uz prethodno uklanjanje nula

Rezultati analize pokazali su da dnevne vrijednosti transakcija ove adrese značajno odstupaju od Benfordove distribucije. Konkretno, dobivena vrijednost MAD (*Mean Absolute Deviation*) iznosi 0.108805, što prema klasifikaciji *benford.analysis* paketa označava „*Nonconformity*" – potpunu nekonformnost s Benfordovim zakonom.

Ovaj rezultat potvrđuje tezu da visoko kontrolirane adrese, poput one Vitalika Buterina, čija aktivnost nije vođena tržišnom logikom, već često uključuje darovanja, prijenose između vlastitih računa ili testne transakcije – ne prate prirodnu distribuciju vodećih znamenki, kakva bi bila očekivana kod stohastičkih i velikih tržišnih sustava.



Prikaz 19: Zbrojene dnevne vrijednosti ETH transakcija *za adresu V. Buterina*

Benfordova analiza dnevnih ETH transakcija adrese Vitalika Buterina pokazuje značajno odstupanje od Benfordove distribucije vodećih znamenki. Grafovi otkrivaju prekomjernu učestalost znamenke 6 i smanjenu učestalost znamenki 1–3, što ukazuje na neprirodan uzorak. Dobivena MAD vrijednost (0.1088) potvrđuje potpunu nekonformnost s Benfordovim zakonom, što je u skladu s karakteristikama ove visoko kontrolirane, netržišne adrese.

U nastavku će biti prikazani i analizirani rezultati za druge adrese – uključujući one za koje se sumnja ili zna da su bile uključene u prevarne aktivnosti radi usporedbe i dodatnog utemeljenja metodološkog pristupa.

3.7.2 Kraken hot wallet

Adresa Kraken Hot Wallet pripada jednoj od najaktivnijih centraliziranih burzi na Ethereum mreži. Takve adrese obično procesuiraju ogroman broj transakcija u ime svojih korisnika,

uključujući kupnje, prodaje i povlačenja sredstava. Analiza ove adrese pruža vrijedan uvid u ponašanje "institucionalnog" aktera koji djeluje kao posrednik između korisnika i blockchaina.

Predviđanje ponašanja

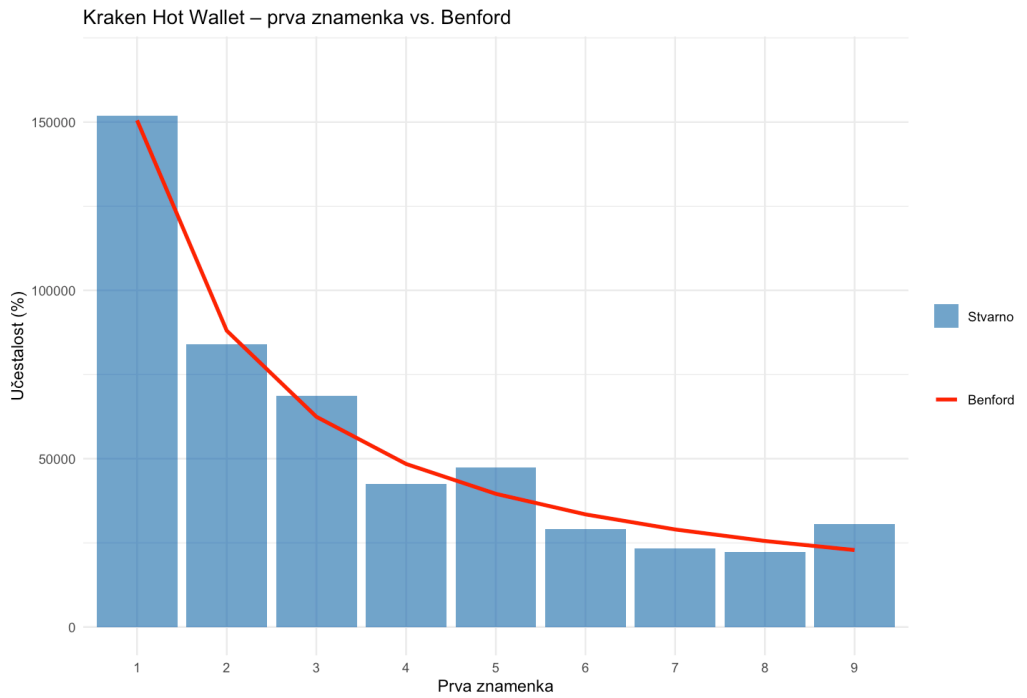
S obzirom na to da burzovne adrese agregiraju i automatizirano obrađuju veliki broj korisničkih transakcija, pretpostavlja se:

- visok stupanj regularnosti
- relativno konzistentne vrijednosti
- slijed Benfordovog zakona, jer veliki broj različitih korisničkih unosa često dovodi do "prirodne" raspodjele znamenki

Rezultati

Rezultati analize za srpanj 2025. potvrđuju ove pretpostavke:

- MAD ≈ 0.0104, što ukazuje na "*acceptable conformity*" vrijednosti transakcija prema Benfordovom zakonu
- Graf distribucije prve znamenke pokazuje oblik vrlo sličan teoretskoj raspodjeli
- χ^2 test daje značajnu p-vrijednost, no to je česta pojava kod vrlo velikih uzoraka



Prikaz 20: Distribucija prve znamenke pojedinačnih transakcijskih vrijednosti (neagregirano) za Kraken hot wallet adresu

Zaključak

Unatoč manjim odstupanjima kod pojedinih znamenki (npr. 5 i 9 su blago precijenjene), transakcije Kraken hot walleta u cjelini prate Benfordov zakon. Ova usklađenost potvrđuje očekivano ponašanje institucionalne adrese s velikim prometom i mnogobrojnim korisnicima. Takve adrese rijetko pokazuju sumnjiva odstupanja jer redovito podliježu regulatornim standardima i unutarnjim kontrolama.

3.7.3 MEV Bot (Maximal Extractable Value)

Iduća analizirana adresa pripada jednom od poznatijih MEV (Maximal Extractable Value) botova na Ethereum mreži. MEV botovi su specijalizirani algoritmi koji automatski skeniraju i manipuliraju redoslijedom transakcija u bloku kako bi ostvarili financijsku dobit - najčešće putem tehnika kao što su *frontrunning* ili *sandwich* napadi. Ova vrsta aktivnosti predstavlja značajan izazov za tržište te je zato korisno analizirati njihove transakcijske obrasce u potrazi za nepravilnostima ili odstupanjima.

Promatrano je razdoblje od 24. travnja 2020. do 8. svibnja 2020.. Fokus je bio isključivo na ERC-20 token transferima, što omogućava detaljnu kvantitativnu obradu iznosa i njihovu usporedbu s predviđanjima prema Benfordovom zakonu.

Predviđanje ponašanja

S obzirom na to da se radi o potpuno automatiziranom algoritmu, očekuje se:

- odsustvo prirodne distribucije znamenki, jer bot ne izvršava nasumične ili ljudske odluke
- velika preciznost i ponavljanje obrazaca u vrijednostima
- odstupanja od Benfordovog zakona, budući da su vrijednosti transakcija rezultat optimizacijskih algoritama, a ne organskog financijskog ponašanja

Rezultati

Rezultati analize pokazuju jasno odstupanje od predviđene Benfordove raspodjele:

- Po danu:

MAD ≈ 0.0717

Konformnost: *Nonconformity*

- Po satu:

  MAD ≈ 0.0214

Konformnost: *Nonconformity*

- Po pojedinačnoj transakciji:

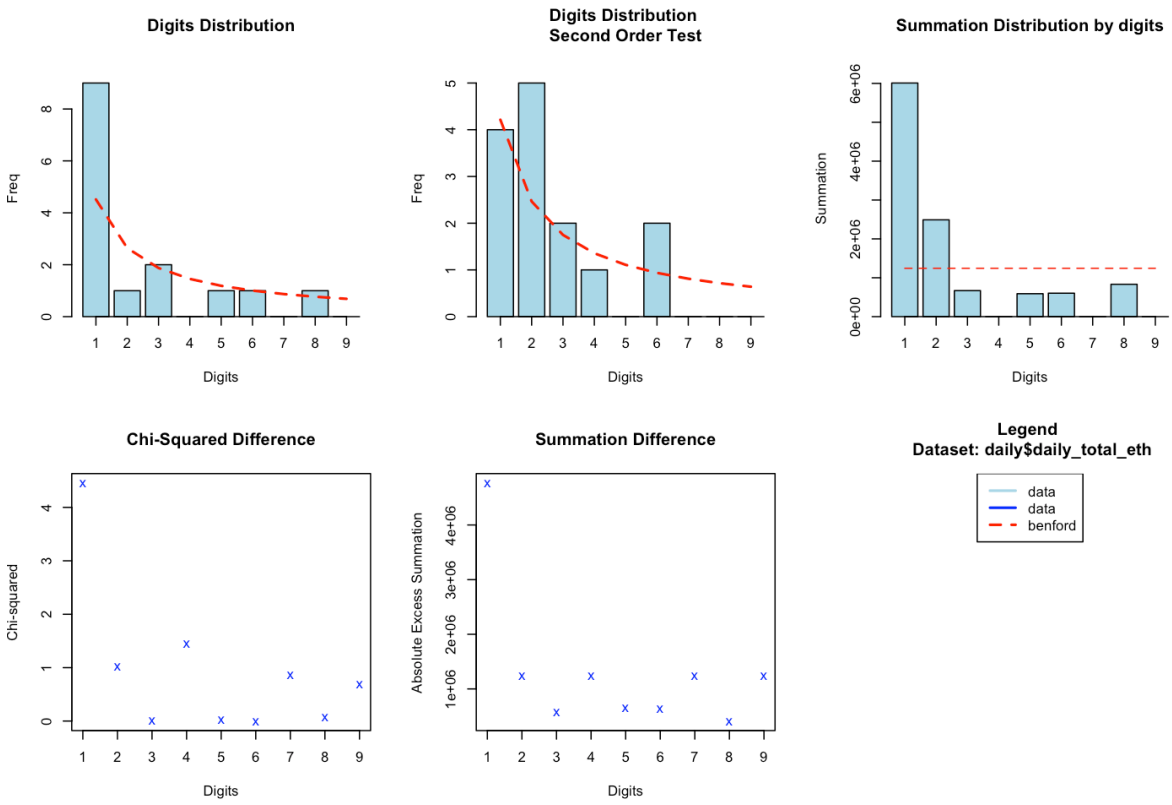
  MAD ≈ 0.0925

  Konformnost: *Nonconformity*

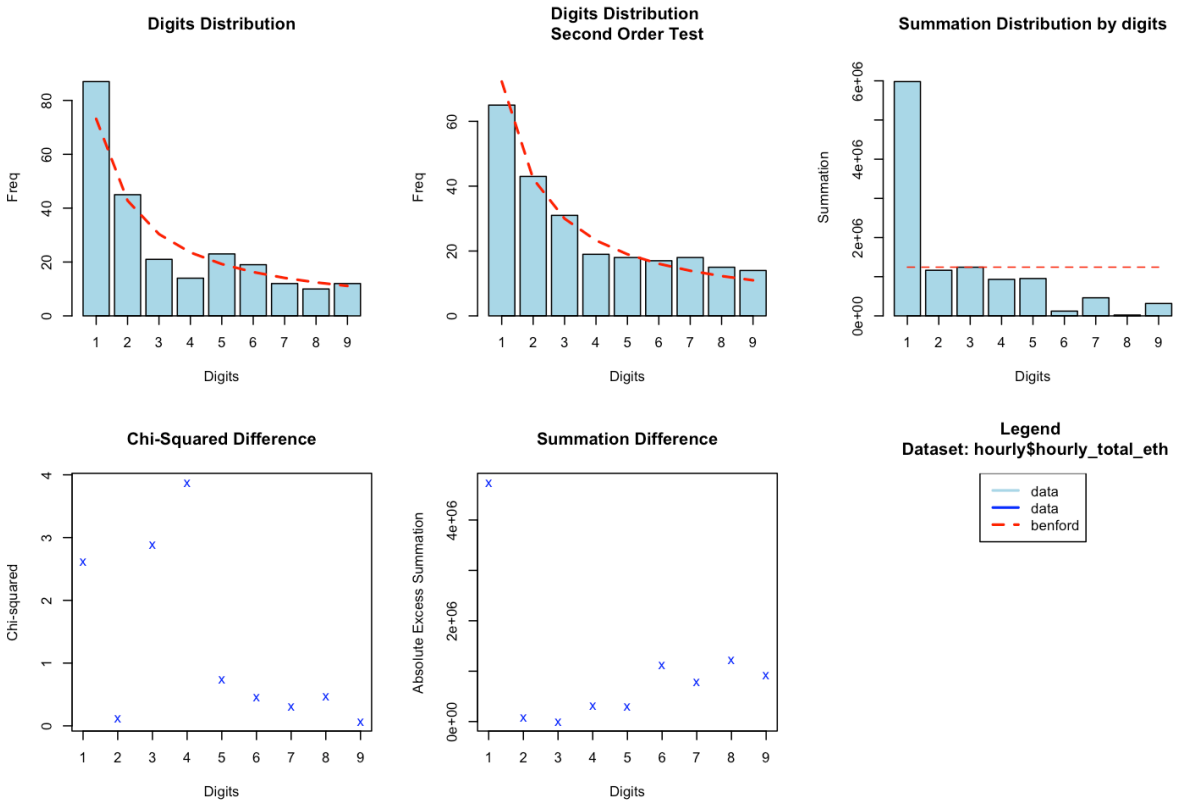
Zaključak

Rezultati potvrđuju početnu pretpostavku da se transakcije ove adrese ne ponašaju u skladu s Benfordovim zakonom, što je i očekivano za adresu kojom upravlja automatizirani bot (uočljivo također na grafovima). Odsustvo ljudskog faktora i uporaba optimizacijskih strategija dovodi do nelinearnih, mehaničkih obrazaca u vrijednostima, što se reflektira i u distribuciji znamenki.

Iako ova analiza ne upućuje nužno na prevarno ponašanje, jasno ukazuje na automatiziranu aktivnost koja odstupa od predviđenih distribucija kod klasičnih korisničkih ili institucionalnih računa. Upravo zato, ovakvi alati su korisni za prepoznavanje sumnjivih obrazaca i za buduće istraživanje tržišnih aktera koji operiraju na granici etičnosti i regularnosti.



Prikaz 21: Benfordova analiza agregiranih vrijednosti po danu za MEV Bot adresu



Prikaz 22: Benfordova analiza agregiranih vrijednosti po satu za MEV Bot adresu

3.7.4 Binance Hot Wallet

Za potrebe analize odabrana je još jedna od najpoznatijih *hot wallet* adresa burze Binance. Riječ je o adresi koja ima izuzetno frekventan promet i koristi se za svakodnevne operacije poput slanja i primanja sredstava između korisnika i burze. Pretpostavka je bila da će, s obzirom na institucionalnu narav adrese i veliki broj legitimnih transakcija, distribucija prve znamenke iznosa transakcija pokazati visoku podudarnost s Benfordovom distribucijom.

Promatrano razdoblje obuhvaća devet dana, od 5. kolovoza 2017. do 14. kolovoza 2017., tijekom kojih je prikupljeno ukupno 2783 transakcije s pozitivnim vrijednostima. Iz svakog iznosa transakcije izdvojena je prva znamenka te je zatim izračunata opažena frekvencija svake od znamenki od 1 do 9. Vizualna usporedba jasno pokazuje da postoji određeni stupanj slaganja - znamenka 1, kao najčešća prema Benfordovom zakonu, doista je i ovdje najzastupljenija s udjelom od 32.99 %, nešto većim od predviđenih 30.1 %. Slično vrijedi i za znamenku 2, dok su neka odstupanja uočena kod znamenki 3 i 5, koje se pojavljuju rjeđe ili češće nego što bi to Benford predviđao.

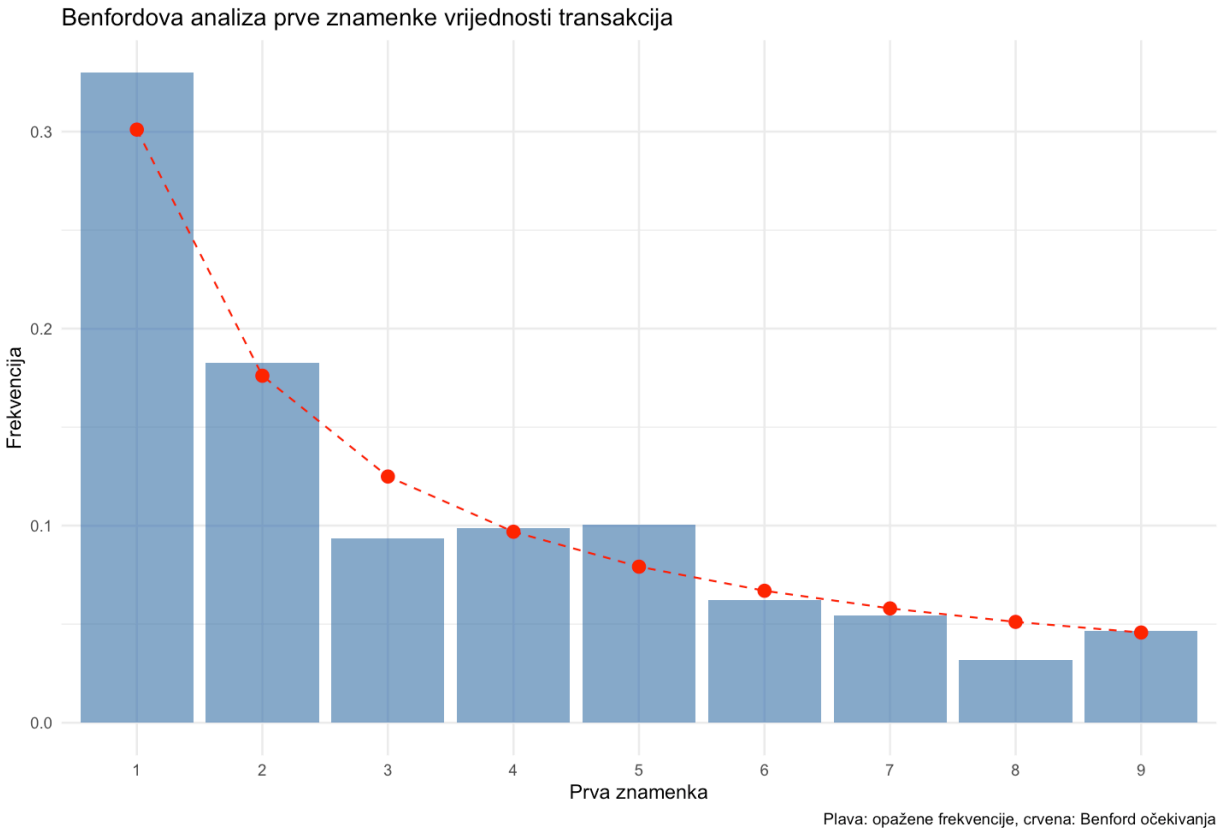
First digit	N	Frequency	Expected
1	707	0,32991134	0,30103
2	391	0,1824545	0,17609126
3	200	0,09332711	0,12493874
4	212	0,09892674	0,09691001
5	215	0,10032664	0,07918125
6	133	0,06206253	0,06694679
7	117	0,05459636	0,05799195
8	68	0,03173122	0,05115252
9	100	0,04666356	0,04575749

Tablica 5: Usporedba empirijske i predviđene distribucije prve znamenke

Kako bi se kvantificirala razina slaganja s Benfordovim zakonom, izračunata je vrijednost MAD, koja u ovom slučaju iznosi 0.0132. Prema klasifikaciji razine podudarnosti, ovaj rezultat upućuje na umjerenu podudarnost s Benfordovim zakonom. Dodatno je proveden i $\underline{\chi^2}$ test koji je dao p-vrijednost manju od 0.000000012, što ukazuje na statistički značajno odstupanje od Benfordove distribucije na razini značajnosti od 5 %. Iako je vizualna podudarnost djelomično prisutna, statistička analiza sugerira da distribucija ipak ne slijedi Benfordov zakon.

Ovakav rezultat može se interpretirati na više načina. S jedne strane, Binance kao centralizirana burza obavlja niz ponavljajućih operacija, što može utjecati na strukturu transakcija i dovesti do odstupanja od prirodne distribucije. S druge strane, moguće je i da su neki od prijenosa interno uvjetovani, odnosno da su tehničke naravi (npr. grupirane isplate korisnicima), što također utječe na raspodjelu prvih znamenki.

Zaključno, iako adresa pokazuje određenu podudarnost s Benfordovim zakonom, posebno kod dominantnih znamenki, potpuna usklađenost izostaje. To je u skladu s pretpostavkom jer se radi o institucionalnoj adresi čije transakcije nisu isključivo rezultat tržišnog ponašanja pojedinaca, već i strukturiranih procesa unutar same burze. Rezultati nam pružaju korištan uvid u obrasce ponašanja ove adrese, ali i potvrđuju da primjena Benfordovog zakona u kriptovalutnom prostoru mora uvijek uzeti u obzir kontekst korištenja analizirane adrese.



Prikaz 23: Raspodjela prve znamenke vrijednosti svake transakcije ETH (bez agregacije) za Binance Hot Wallet adresu

3.7.5 Fake MyEtherWallet scam (phishing adresa)

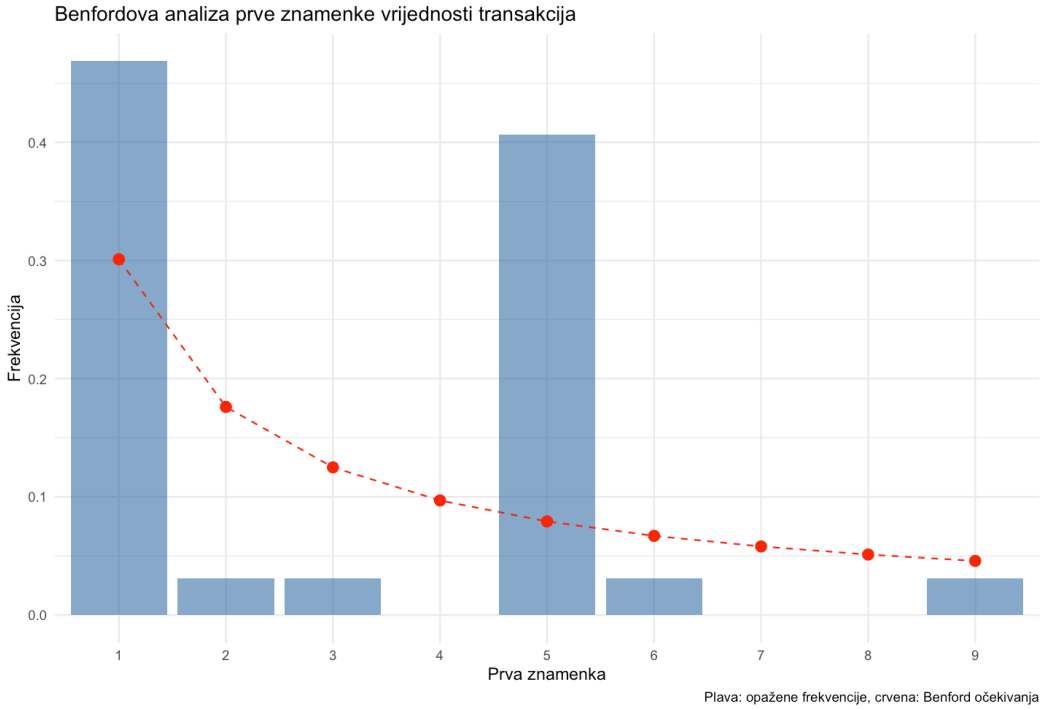
Sljedeći korak analize uključivao je proučavanje Ethereum adrese koja je u kripto svijetu poznata kao *phishing* adresa povezana s lažnim servisom *MyEtherWallet*. Ova adresa korištena je za prevarne aktivnosti u sklopu *phishing* kampanja s ciljem krađe sredstava korisnika koji su pogrešno vjerovali da komuniciraju sa službenom *MyEtherWallet* stranicom. Upravo zbog tog konteksta, odabrana je kao idealan kandidat za pokušaj detekcije sumnjivih obrazaca pomoću Benfordovog zakona.

Analiza obuhvaća transakcije u kojima su na ovu adresu uplaćeni ETH iznosi u razdoblju od 18. srpnja 2017. do 20. ožujka 2025., odnosno u preko sedam godina aktivnosti. Cilj je bio provjeriti pojavljuju li se prve znamenke iznosa transakcija u skladu s Benfordovim zakonom, koji predviđa da će znamenka 1 biti najčešća (oko 30 %), a znamenke veće od 5 pojavljivati se sve rjeđe.

Rezultati analize pokazuju značajno odstupanje od predviđene Benfordove distribucije. Najčešće se kao prva znamenka pojavljuje broj 1, što je u skladu s pretpostavkom, ali također zapanjujuće često pojavljuje se znamenka 5, čak više od pet puta češće od onoga što Benfordova distribucija predviđa za tu znamenku (40.6 % naspram predviđenih 7.9 %). Ostale znamenke javljaju se vrlo rijetko.

Statistički test koji daje izrazito nisku p-vrijednost ($p < 0.000000001$) te MAD vrijednost (0.1099) omogućuju da s velikom sigurnošću zaključimo kako distribucija nije u skladu s Benfordovim zakonom.

U kontekstu činjenice da se radi o *phishing* adresi, ovi rezultati dodatno pojačavaju sumnju da su transakcije bile namjerno strukturirane ili kontrolirane, možda čak i automatizirane, kako bi se prikrile ili lažno predstavile određene aktivnosti. Visoka frekvencija određene znamenke (poput broja 5) može upućivati na unificirani ili skriptirani obrazac uplata, što dodatno naglašava važnost automatizirane detekcije ovakvih odstupanja u sustavima nadzora blockchain prometa.



Prikaz 24: Usporedba opaženih i predviđenih frekvencija prve znamenke vrijednosti pojedinačnih ETH transakcija za lažnu MyEtherWallet adresu

Zaključno, ova analiza pokazuje kako Benfordov zakon može poslužiti kao brza i učinkovita forenzička metoda za uočavanje neuobičajenih obrazaca transakcija na blockchain adresama,

osobito kada postoji sumnja u legitimnost aktivnosti. Iako metoda ne može identificirati vrstu prevare, pruža vrijedan statistički signal koji opravdava dodatnu istragu.

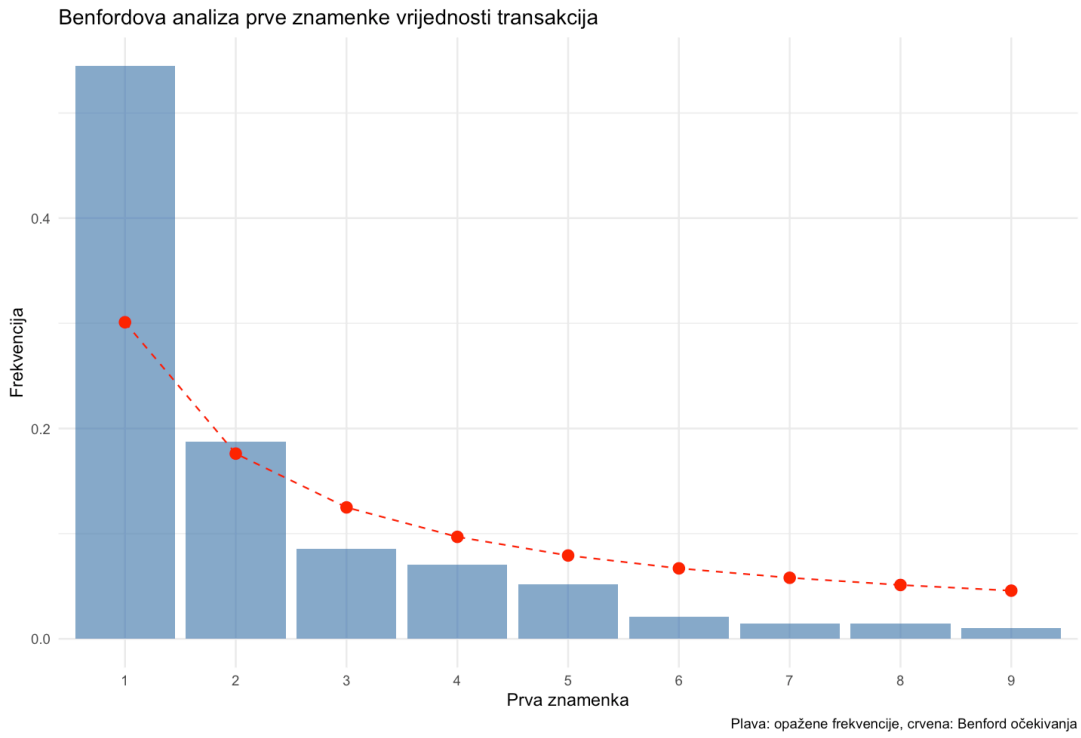
3.7.6 Giveaway Scam

Razlog za analizu upravo ove adrese proizlazi iz činjenice da je riječ o jednoj od najpoznatijih adresa povezanih s *giveaway scamovima* na Twitteru. Ova adresa često se koristila u prevarama u kojima su hakeri preuzimali identitete poznatih osoba, najčešće Elona Muska, i lažno obećavali višestruki povrat korisnicima koji pošalju određenu količinu kriptovalute. Analiza ovakvih adresa može pokazati postoje li obrasci u financijskom ponašanju koji se razlikuju od "normalnog" prometa i tako poslužiti kao alat za detekciju sumnjivih aktivnosti.

U ovom slučaju očekujemo da iznosi transakcija neće pratiti prirodni raspored koji se inače pojavljuje u stvarnim financijskim podacima. Ako je aktivnost na adresi nastala kao posljedica manipulacije ili prevare, postoji mogućnost da transakcije neće slijediti pretpostavljenu raspodjelu, nego će biti namještene tako da imaju ponavljajuće obrasce.

Podaci su prikupljeni za razdoblje od 20. kolovoza 2016. do 1. prosinca 2018. i uključuju ukupno 509 transakcija s pozitivnim vrijednostima. Za svaku transakciju izdvojena je prva znamenka vrijednosti izražene u etherima, a zatim su uspoređene opažene frekvencije sa statistički očekivanima prema Benfordovu zakonu.

Rezultati su pokazali značajno odstupanje. Više od 54 % transakcija započinje znamenkom 1, dok se prema Benfordovu zakonu to predviđa u oko 30 % slučajeva. Ostale znamenke također su bile nepravilno zastupljene, pri čemu se veće znamenke (6–9) pojavljuju značajno rjeđe nego što bi trebalo. Statistička provjera pomoću χ^2 testa dala je izrazito nisku p-vrijednost ($< 2.2e\text{-}16$), što potvrđuje da opaženi podaci ne prate Benfordovu distribuciju. Dodatno, izračunata vrijednost MAD iznosi 0.0566, što ukazuje na loše slaganje s Benfordovim zakonom.



Prikaz 25: Frekvencije pojavljivanja prve znamenke u vrijednostima ETH transakcija, uspoređujući opažene frekvencije (plavo) s Benfordovim teorijskim vrijednostima (crveno) za Giveaway Scam adresu

Zaključno, analiza potvrđuje da obrasci u transakcijama ove adrese odstupaju od onoga što bismo očekivali kod legitimne financijske aktivnosti. Ova vrsta odstupanja, u kombinaciji s poznatom reputacijom adrese i njezinom povezanosti s prevarama, dodatno potvrđuje sumnju da je riječ o neautentičnom i manipuliranom ponašanju. Benfordova analiza u ovom kontekstu pokazuje se kao jednostavan, ali učinkovit alat za rano otkrivanje neuobičajenih aktivnosti na blockchainu.

Dodatno, uz analizu vrijednosti transakcija u Etheru, provedena je i zasebna analiza ERC-20 token transakcija za istu adresu, s ciljem proširenja uvida u ponašanje adrese i potencijalne nepravilnosti. ERC-20 tokeni predstavljaju velik broj različitih kriptovaluta koje funkcioniraju na Ethereum mreži, a njihova analiza može otkriti još šire obrasce ponašanja korisnika ili automatiziranih sustava (botova) iza adrese.

Podaci obuhvaćaju razdoblje od 21. srpnja 2017. do 11. srpnja 2025., dakle gotovo osam godina aktivnosti. Za razliku od prethodne analize gdje su promatrane samo transakcije u Etheru, ovdje je analizirano kretanje vrijednosti ERC-20 tokena. Analizirani su svi pozitivni iznosi.

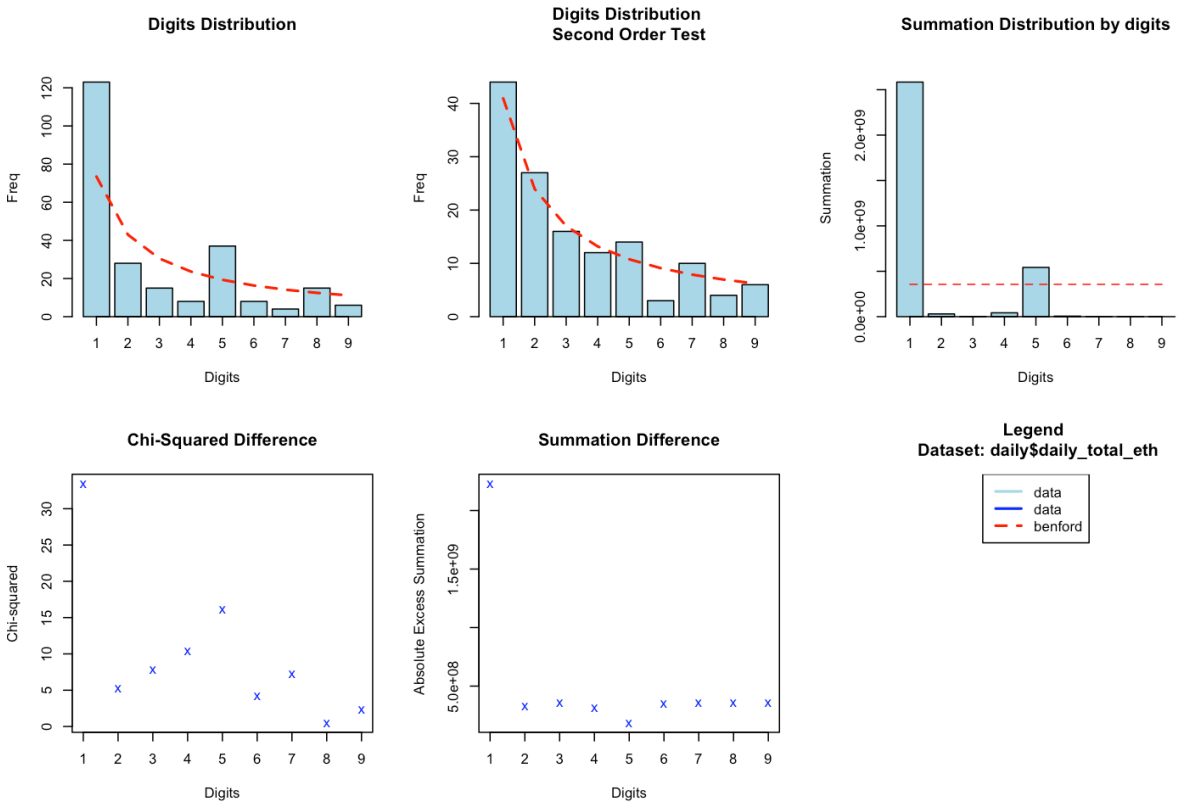
Kako bi se povećala preciznost analize, Benfordov zakon primijenjen je na tri razine:

1. Ukupni iznosi po danu
2. Ukupni iznosi po satu
3. Pojedinačne vrijednosti svake transakcije

Rezultati su sljedeći:

Benford po danu:

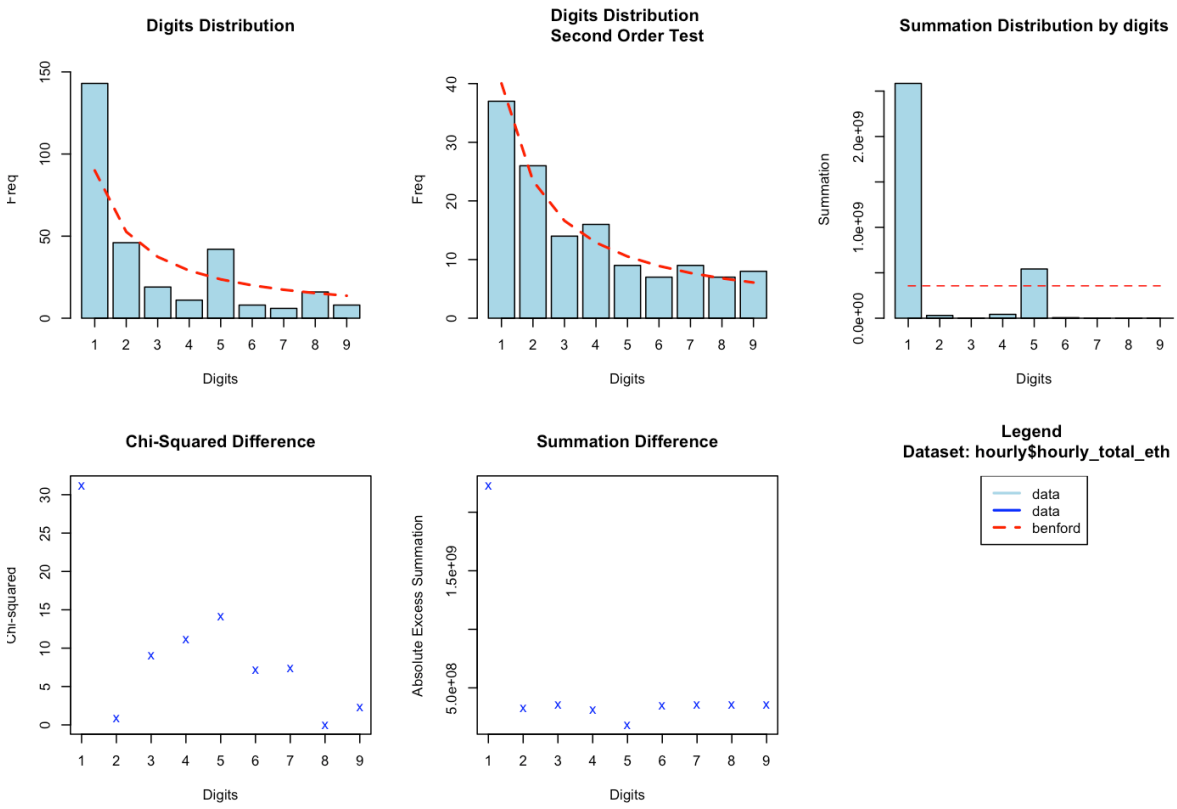
Dobivena MAD vrijednost iznosi 0.0635, što ukazuje na nekonformnost s Benfordovim zakonom. To znači da dnevna distribucija iznosa ne slijedi predviđene obrasce, što može upućivati na umjetno generirane ili manipulirane transakcije.



Prikaz 26: Dnevna distribucija iznosa ERC-20 token transakcija za Giveaway Scam adresu

Benford po satu:

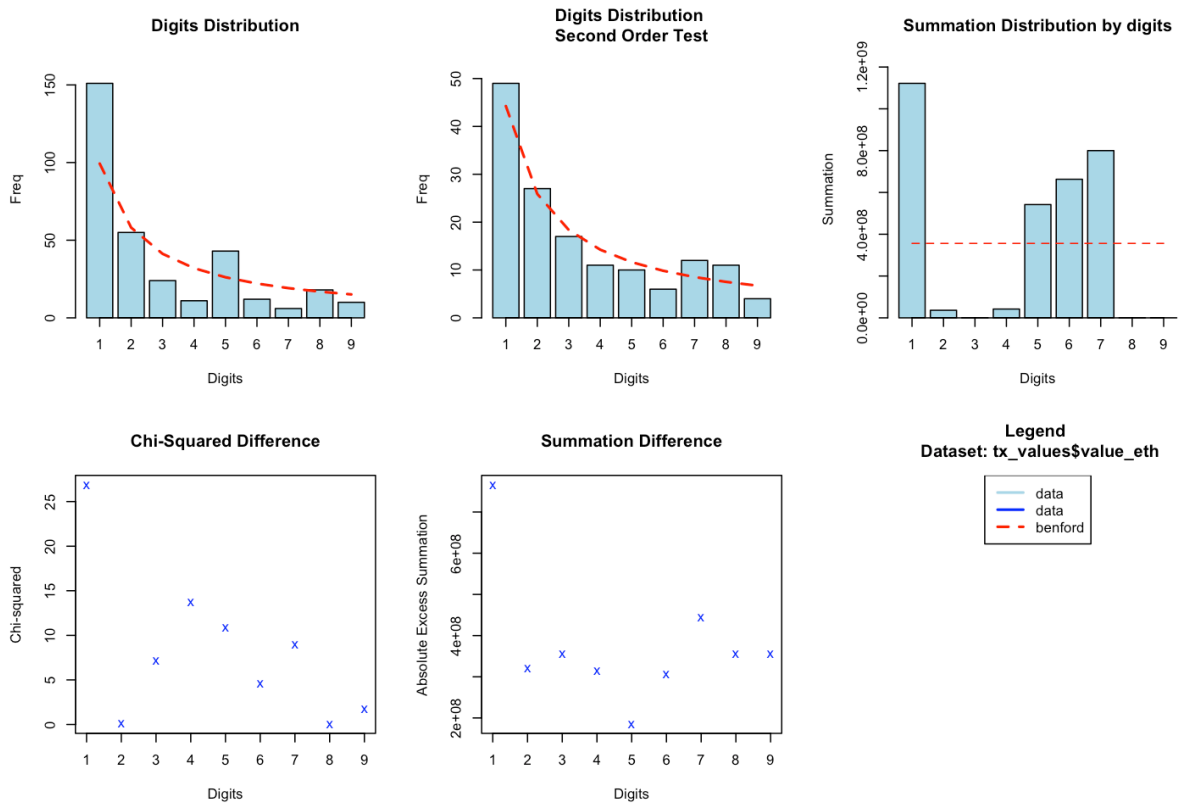
Još jedno mjerenje pokazuje MAD vrijednost 0.0535, također označeno kao nekonformno. S obzirom na to da bi transakcije u satnom intervalu trebale imati prirodniju raspodjelu kod redovitih aktivnosti korisnika, ovakav rezultat dodatno potvrđuje sumnju u neregularnost.



Prikaz 27: Satna distribucija iznosa ERC-20 token transakcija za Giveaway Scam adresu

Benford po vrijednosti transakcija:

Promatrajući svaku pojedinačnu transakciju, dobiven je MAD od 0.0469, što je niže od dnevnog i satnog prosjeka, ali i dalje dovoljno visoko da bude klasificirano kao nekonformno.



Prikaz 28: Distribucija iznosa vrijednosti transakcija ERC-20 token transakcija za Giveaway Scam adresu

Dakle, u sve tri razine analize ERC-20 tokena uočena su statistički značajna odstupanja od prirodnih obrazaca koje predviđa Benfordov zakon. Kao i kod Ether transakcija, i ovdje je dominantan uzorak koji upućuje na moguću automatizaciju, namještanje ili skriptirano ponašanje – što se poklapa s poznatim obrascima ponašanja adresa uključenih u prevare.

Zanimljivo je primijetiti da se aktivnosti na ovoj adresi nastavljaju sve do sredine 2025. godine, iako su najintenzivniji valovi giveaway prevara zabilježeni ranije. To može ukazivati ili na dugoročne manipulacije kroz druge tokene, ili na ponovnu aktivaciju adrese u novim pokušajima prevare.

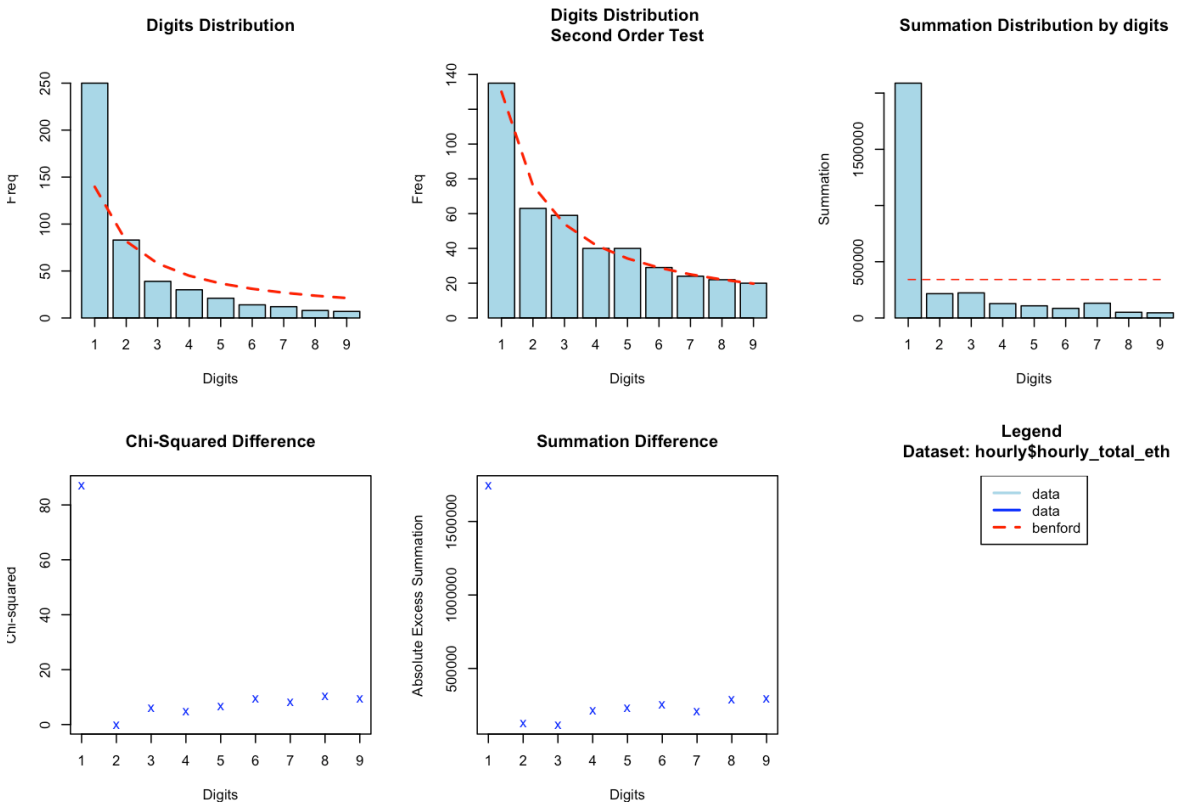
Kombinacijom analize Ether i ERC-20 transakcija dobiva se snažnija potvrda da ova adresa pokazuje ponašanje koje značajno odstupa od prirodnog financijskog prometa. Iako Benfordov zakon sam po sebi nije dokaz prevare, u kontekstu poznate povijesti adrese, ponavljajuće devijacije od predviđene raspodjele predstavljaju ozbiljan indikator za daljnju istragu.

3.7.7 Fake ICO scam (Lažna ICO kampanja)

Iduće, analizirana je Ethereum adresu povezana s lažnom ICO kampanjom. Radi se o slučaju u kojem je pokretač projekta putem inicijalne ponude tokena (*Initial Coin Offering* – ICO) prikupio sredstva od investitora, bez namjere razvoja stvarnog proizvoda. Adresa je poznata u blockchain zajednici kao primjer projekta s elementima prevare, zbog čega predstavlja dobar kandidat za forenzičku analizu transakcija.

Podaci su prikupljeni korištenjem Etherscan API-ja u razdoblju od 20. kolovoza 2016. do 10. svibnja 2024. U tom razdoblju zabilježene su sve „normalne“ (tj. ETH) transakcije povezane s analiziranom adresom. Ponovno je izvršena agregacija po danima i satima, kao i analiza pojedinačnih vrijednosti transakcija, kako bi se Benfordov zakon testirao na više vremenskih razina.

Rezultati su pokazali značajna odstupanja na svim razinama. U agregaciji po danima izračunata je vrijednost MAD = 0.0200, uz procjenu "*Nonconformity*", što znači da dnevne vrijednosti transakcija ne slijede predviđenu raspodjelu. Kod analize po satima odstupanje je bilo još izraženije, s vrijednošću MAD = 0.0535, što dodatno upućuje na neprirodan uzorak aktivnosti. Na razini pojedinačnih transakcija također je utvrđena neusklađenost s Benfordovim zakonom (MAD = 0.0542). Ovi rezultati ukazuju na moguće manipulacije transakcijama, programirano slanje sredstava ili pokušaje prikrivanja stvarnog toka novca.



Prikaz 29: Benfordova analiza normalnih transakcija po satu za adresu lažne ICO kampanje

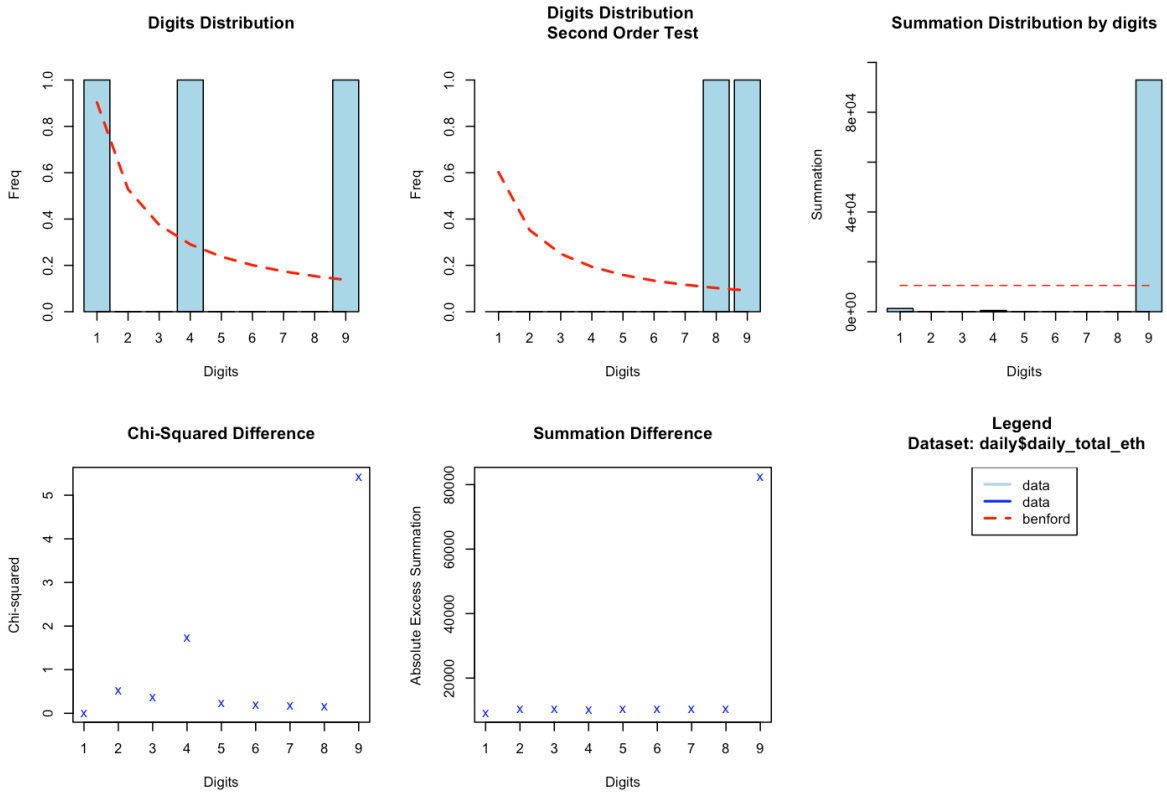
Zaključno, iako ova analiza sama po sebi ne može potvrditi postojanje prevare, ona jasno identificira anomalije koje zaslužuju daljnju istragu. Promatrani podaci u trajanju od gotovo osam godina pružaju dovoljno konteksta da se zaključci mogu smatrati relevantnima, a u slučaju adrese povezane s lažnom ICO kampanjom rezultati pokazuju jasne znakove nepravilnosti.

3.7.8 Fake Uniswap Airdrop

Promatrana adresa je povezana s poznatim slučajem lažnog Uniswap airdropa. Riječ je o tipu prevare koji se često temelji na socijalnom inženjeringu, gdje korisnici dobivaju pozive na sudjelovanje u besplatnoj raspodjeli tokena (tzv. *airdrop*), no pritom su preusmjereni na sumnjive pametne ugovore ili im se kriptovalute izravno kradu iz novčanika. Adresa iz ovog slučaja korištena je u više navrata za zaprimanje i slanje sredstava kao dio tzv. *phishing* i *airdrop scam* kampanja. Upravo zbog te sumnjive reputacije odabrana je za forenzičku analizu, s ciljem utvrđivanja postoje li statistički značajna odstupanja koja bi dodatno potvrdila nepravilnosti u njenom transakcijskom obrascu.

Analiza je provedena na uzorku svih dostupnih „normalnih“ (ETH) transakcija. Podaci pokrivaju vrlo kratko, ali intenzivno razdoblje - od 7. siječnja 2018. do 9. siječnja 2018. Takvo kratko, ali vrlo aktivno razdoblje (3374 transakcija) karakteristično je za prevare poput lažnih airdropova, gdje se veliki broj transakcija odvija u kratkom vremenu s ciljem iskorištavanja trenutne pažnje žrtava.

Dobiveni rezultati pokazuju značajno odstupanje u svim aspektima. Kod agregacije po danima dobiven je iznimno visok MAD od 0.1236, što jasno ukazuje na neusklađenost s Benfordovim zakonom i snažno sugerira neprirodan obrazac dnevnih transakcija. Kod analize po satima dobiven je MAD od 0.0778, što je također daleko iznad granice konformnosti i ukazuje na potencijalno automatizirano slanje sredstava u određenim vremenskim intervalima. Na razini pojedinačnih transakcija zabilježen je MAD od 0.0264, što je nešto blaže odstupanje, no i dalje unutar domene neusklađenosti, što je posebno važno jer obuhvaća konkretne vrijednosti koje su slane ili zaprimane.



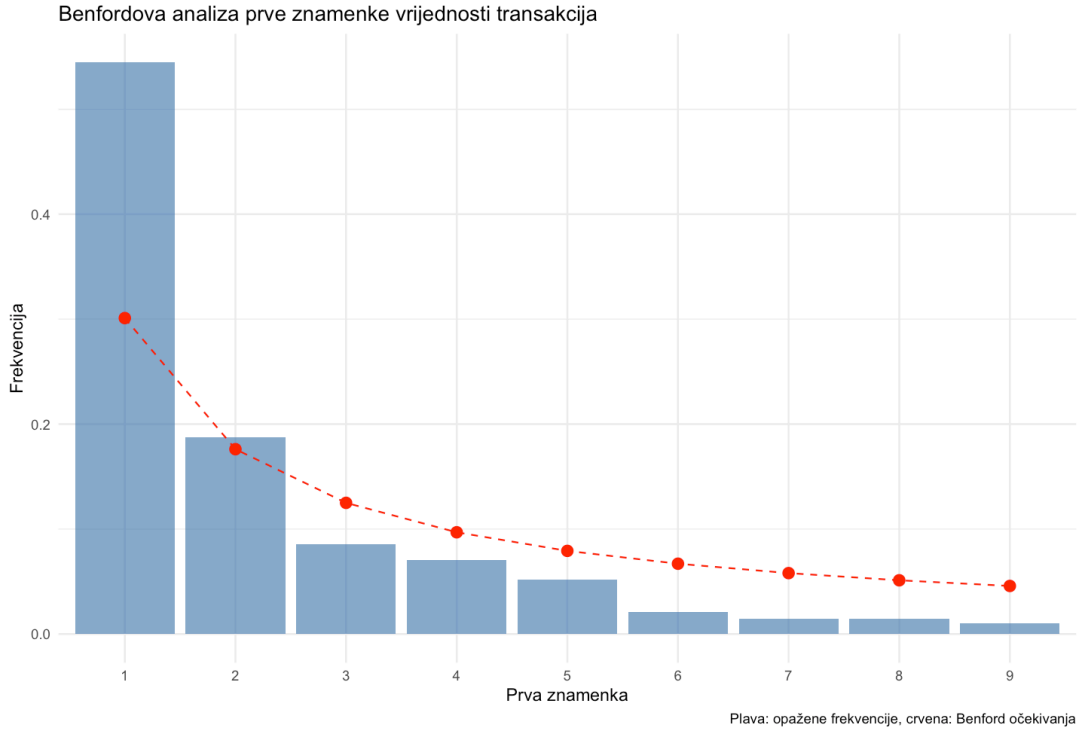
Prikaz 30: Dnevna Benfordova analiza transakcija za lažnu Uniswap Airdrop adresu

Rezultati jasno ukazuju da transakcijska aktivnost povezane adrese ne slijedi prirodnu distribuciju očekivanu kod legitimnih i organskog porijekla financijskih podataka. Unatoč kratkom

razdoblju promatranja, podaci su dovoljno koncentrirani da se dobije jasna slika o obrazcu ponašanja, koji u ovom slučaju pokazuje sve značajke nepravilnosti i potencijalne prevare. Stoga se može zaključiti da Benfordova analiza, i u ovako specifičnim okolnostima, pruža korisne uvide za rano otkrivanje sumnjivih aktivnosti na blockchainu. U budućnosti bi takav pristup mogao biti ugrađen u nadzorne sustave za automatizirano prepoznavanje prevarnih uzoraka unutar decentraliziranih mreža.

3.7.9 PlusToken (jedna od najvećih Ponzi shema)

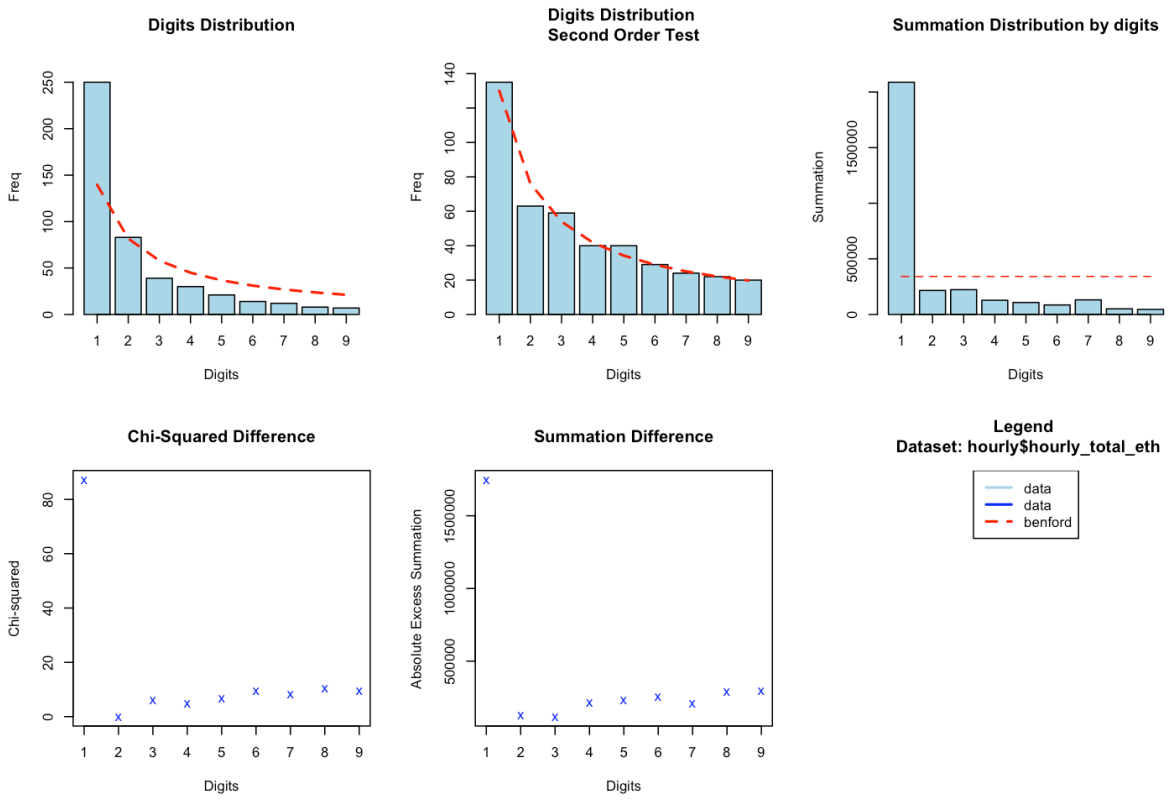
PlusToken adresa je poznata kao jedna od najvećih kriptovalutnih *Ponzi shema* u povijesti. Odabrana je povezana adresa za koju je poznato da je primala i prosljeđivala znatne količine sredstava u sklopu iste prevare. Cilj je bio ispitati koliko se uzorak transakcija koje ova adresa generira uklapa u pretpostavke prema Benfordovom zakonu. Analizom se očekivalo otkriti postoje li značajna odstupanja od Benfordove distribucije, što bi dodatno potvrdilo sumnju u nepravilne obrasce ponašanja. Podaci obuhvaćaju razdoblje od 21. kolovoza 2016. do 5. listopada 2024., s ukupno 509 transakcija. Rezultati pokazuju ekstremnu dominaciju znamenke 1 (54.47 % transakcija), znatno iznad teorijske vjerojatnosti od 30.10 %. Ukupna odstupanja potvrđena su χ^2 testom, čija vrijednost iznosi 165.88 sa p-vrijednošću manjom od 2.2e-16, što upućuje na izuzetno statistički značajnu razliku između predviđene i opažene raspodjele. Također, MAD vrijednost iznosi 0.0566, što se kategorizira kao slabo slaganje s Benfordovim zakonom, dodatno potvrđujući sumnjivu prirodu transakcija.



Prikaz 31: Usporedba opaženih frekvencija prve znamenke vrijednosti transakcija s predviđenim frekvencijama prema Benfordovom zakonu za PlusToken adresu

Na temelju ovih rezultata može se zaključiti da analizirana adresa generira transakcije koje znatno odstupaju od prirodnih distribucija, što je u skladu s prethodnim sumnjama i dostupnom dokumentacijom o povezanosti s Ponzi shemom.

U svrhu produbljivanja prethodne analize provedena je dodatna evaluacija transakcija primjenom Benfordove analize na različite vremenske rezolucije i agregirane vrijednosti transakcija, sada koristeći R paket *benford.analysis*. Dok se inicijalna analiza fokusirala isključivo na raspodjelu prve znamenke pojedinačnih transakcija, ova faza analize ponovno je proširena na agregirane podatke po danima i satima, s ciljem dublje detekcije nepravilnosti u obrascima protoka sredstava. Prvo je analizirana ukupna vrijednost transakcija po danu, pri čemu je dobivena MAD vrijednost od 0.0200, što prema standardima Benfordove metode odgovara nekonformnosti. Nadalje, slična analiza provedena je i po satima, gdje je dobivena još izraženija devijacija - MAD iznosi 0.0534, također označena kao nekonformnost, što ukazuje na neregularan raspored vrijednosti transakcija kroz kraće vremenske intervale. Konačno, ponovno je primijenjena Benfordova analiza na sve pojedinačne vrijednosti transakcija, ali sada korištenjem formalnog *benford()* pristupa umjesto vlastitog računa frekvencija, pri čemu je potvrđena prethodna devijacija s MAD vrijednošću od 0.0542, što dodatno učvršćuje raniji zaključak o odstupanju.



Prikaz 32: Benfordova evaluacija transakcija po satu koristeći paket benford.analysis za Plus-Token adresu

Svi rezultati, neovisno o agregacijskoj razini (dnevno, satno ili pojedinačno), ukazuju na to da distribucije ne prate Benfordov zakon, što dodatno potvrđuje sumnju u neregularne aktivnosti povezane s ovom adresom. Podaci obuhvaćaju razdoblje od 21. kolovoza 2016. do 5. listopada 2024., što osigurava dovoljno dugačko i reprezentativno vremensko pokriće za donošenje statistički relevantnih zaključaka.

3.8.1 Primjena automatizirane analize i interpretacija rezultata

U završnoj fazi istraživanja razvijen je vlastiti R skriptni sustav za automatizirani dohvat, obradu i analizu transakcijskih podataka s Ethereum mreže. Analiza je testirana na skupu podataka korištenom u prvoj fazi istraživanja (*transaction_dataset* preuzet s platforme Kaggle). Nakon što su podaci očišćeni i filtrirani, izvršena je Benfordova analiza na temelju prve značajne znamenke. Za svaku adresu izračunata je vrijednost MAD, koja služi kao glavni kriterij za ocjenu odstupanja od Benfordove distribucije. Na temelju preporučenih pragova u literaturi, adresama je dodijeljena jedna od sljedećih kategorija:

- **Strong conformity** (jako podudaranje)
- **Moderate conformity** (umjereno podudaranje)
- **Weak conformity** (slabo podudaranje)
- **Nonconformity** (nepodudaranje)

Ukupno je analizirano 3.513 adresa. Od tog broja, 26.16 % adresa (n = 919) klasificirano je kao nepodudarno s Benfordovim zakonom, što može ukazivati na potencijalno neprirodnu distribuciju vrijednosti transakcija i posljedično – sumnjivu aktivnost. Ostatak se raspodijelio na sljedeći način:

- **Strong conformity**: 657 adresa
- **Moderate conformity**: 897 adresa
- **Weak conformity**: 1.040 adresa

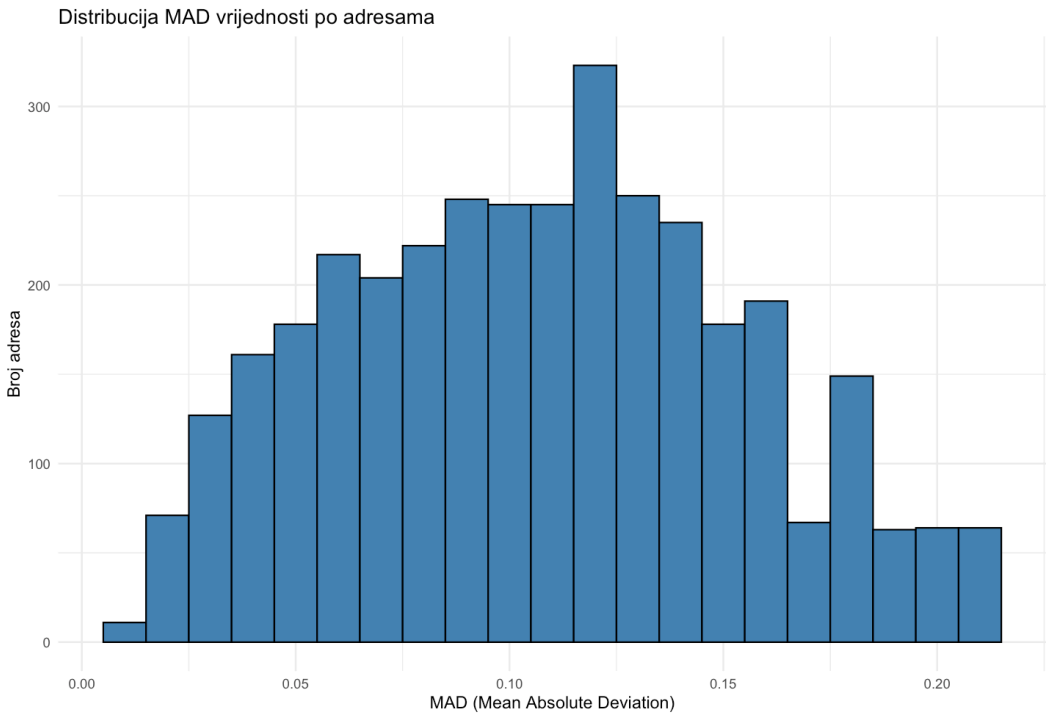
Dodatna statistička analiza pokazala je da su transakcije označene kao nepodudarne prosječno imale veće iznose i veću varijabilnost, dok su one s jakim podudaranjem bile bliže predviđenoj raspodjeli.

Ovi rezultati ne predstavljaju direktan dokaz o zlonamjernoj aktivnosti, ali upućuju na adrese koje bi mogle biti predmet detaljnije istrage, pogotovo ako su povezane s drugim indikatorima rizika (npr. povezanost s poznatim prevarantskim entitetima ili neuobičajeni obrasci ponašanja).

3.8.2 Vizualna interpretacija rezultata analize

Kako bi se dodatno naglasile razlike između sumnjivih i nesumnjivih računa te potvrdila opravdanost primjene Benfordove analize na blockchain transakcije, konstruirano je pet grafova koji zajedno tvore preglednu sliku odnosa između vrijednosti MAD, broja transakcija i kategorizacije računa.

Graf 1: Distribucija MAD vrijednosti po adresama

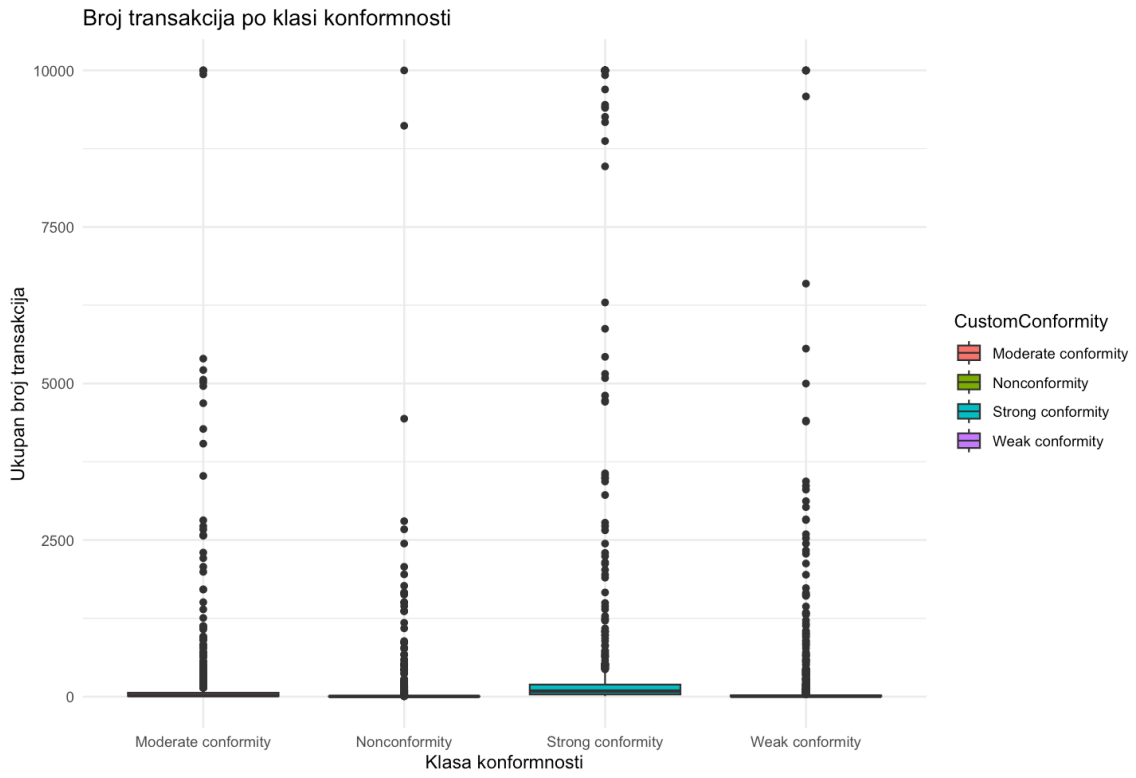


Prikaz 33: Distribucija MAD vrijednosti po adresama za automatizirani sustav

Prvi graf prikazuje histogram raspodjele MAD vrijednosti po analiziranim adresama. MAD mjeri odstupanje distribucije prve znamenke vrijednosti transakcija od idealnog Benfordovog obrasca.

Većina adresa ima MAD vrijednosti niže od 0.15, što ukazuje na relativno dobru sukladnost s Benfordovim zakonom. Manji broj adresa pokazuje veća odstupanja, što može biti indikator neprirodnih obrazaca u transakcijama. Ovaj graf koristimo kako bismo dobili uvid u globalnu distribuciju odstupanja i identificirali potencijalne outliere.

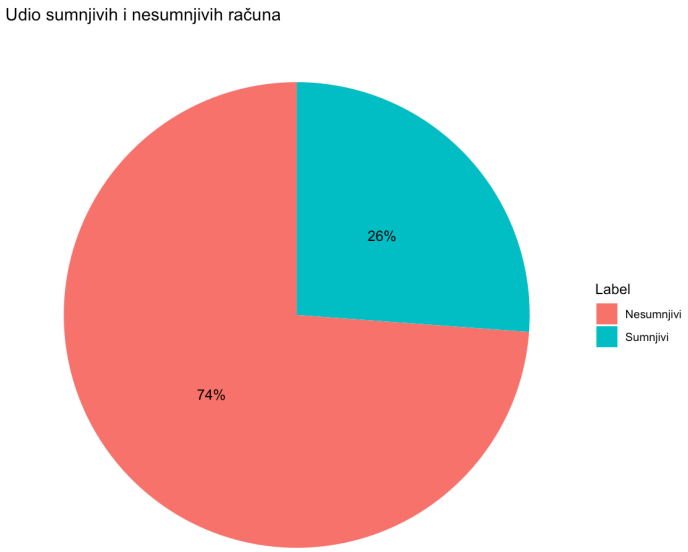
Graf 2: Broj transakcija po klasi konformnosti



Prikaz 34: Kutijasti dijagrami broja transakcija po klasi konformnosti za automatizirani sustav

Ovaj kutijasti dijagram prikazuje distribuciju ukupnog broja transakcija za adrese razvrstane prema vlastito definiranim klasama konformnosti (*Strong, Moderate, Weak, Nonconformity*). Graf pokazuje da adrese s visokom konformnošću (posebno *Strong conformity*) često imaju veći broj transakcija, dok su adrese koje odstupaju od Benfordovog zakona (*Nonconformity*) prisutne u manjem broju i s manjim rasponom aktivnosti. Ovo je važan nalaz jer pokazuje da velik broj transakcija ne implicira nužno sumnjivo ponašanje, već naprotiv – može biti indikator prirodnog, legitimnog ponašanja (što je već pokazano u početnoj fazi istraživanja).

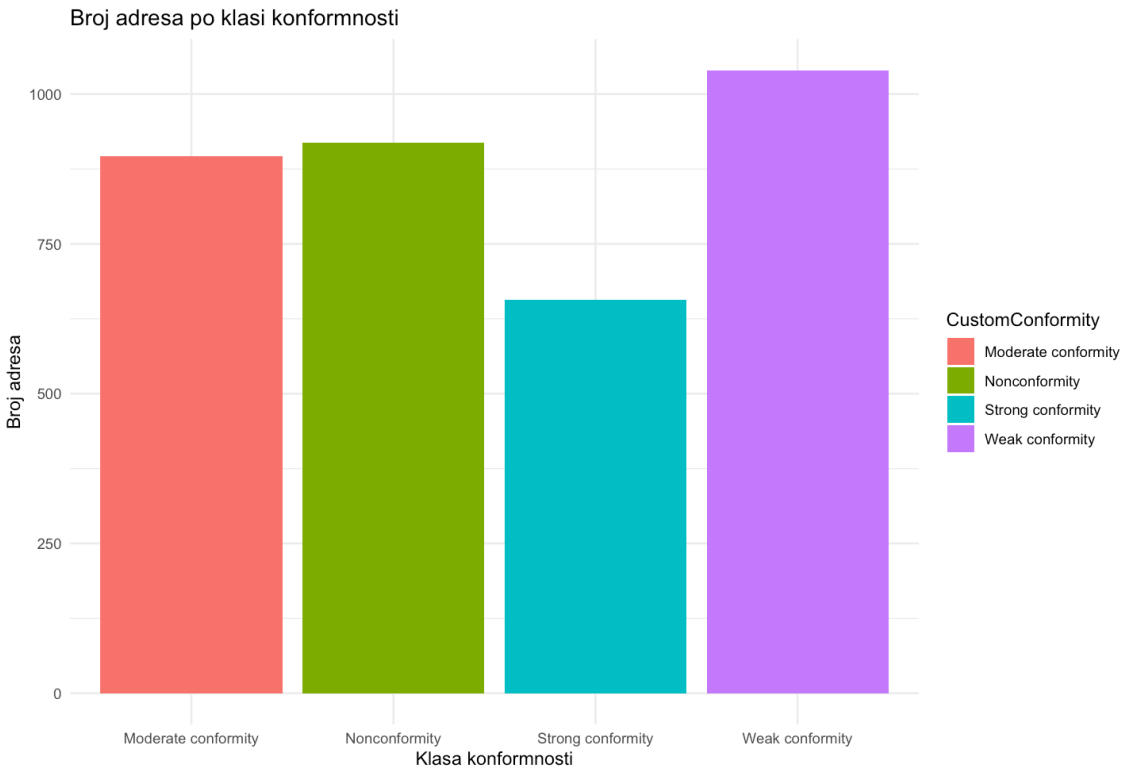
Graf 3: Udio sumnjivih i nesumnjivih računa (pie chart)



Prikaz 35: Pie chart udjela sumnjivih i nesumnjivih računa za automatizirani sustav

Pita dijagram prikazuje relativan udio adresa označenih kao "Sumnjive" (*Nonconformity*) i "Nesumnjive" (ostale klase).

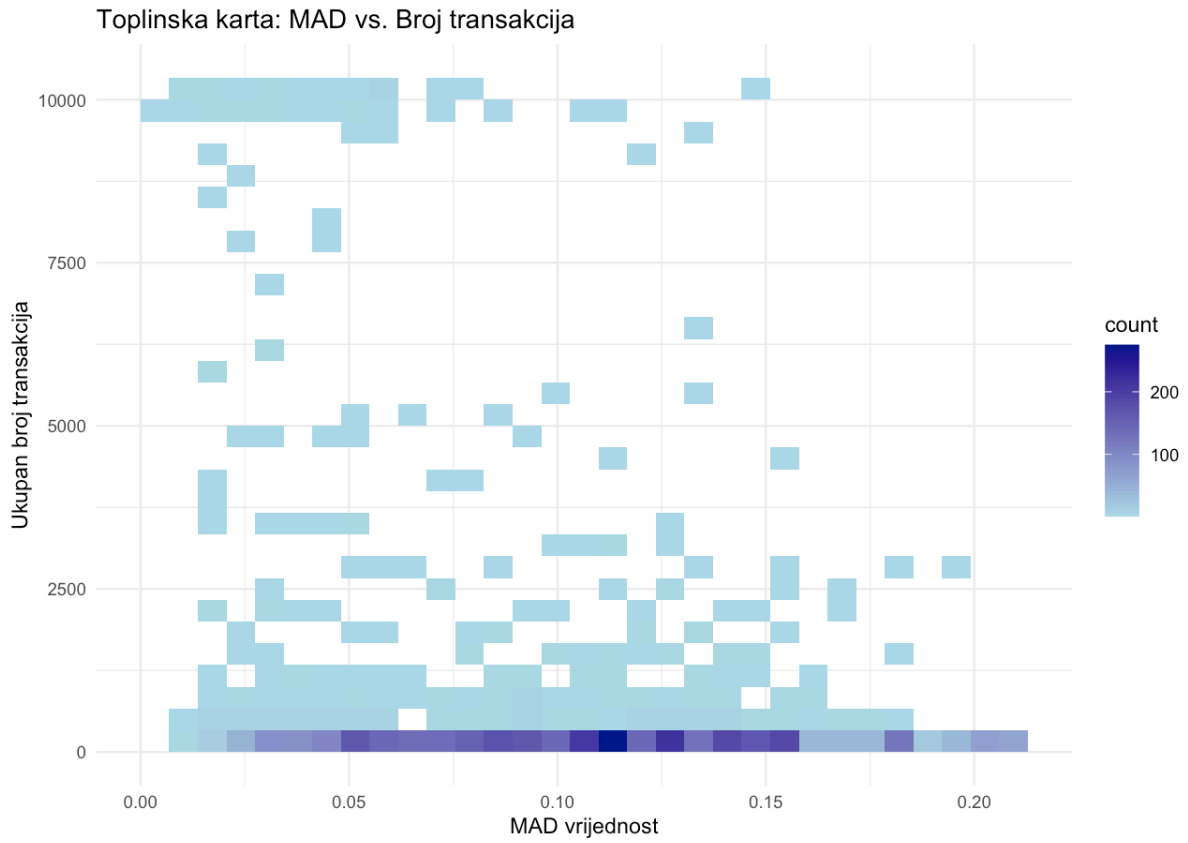
Graf 4: Broj adresa po klasi konformnosti



Prikaz 36: Stupičasti dijagram broja adresa po klasi konformnosti za automatizirani sustav

Ovaj stupčasti graf prikazuje broj adresa po pojedinoj klasi konformnosti prema MAD vrijednostima. Najviše adresa spada u klasu *Weak conformity*, zatim slijede *Nonconformity*, *Moderate*, te *Strong conformity*. Ravnoteža među klasama sugerira da Benfordova distribucija nije savršeno zadovoljena za sve račune, ali istovremeno se ne vidi ekstremna dominacija sumnjivih adresa, što je pozitivan pokazatelj za cjelokupni uzorak.

Graf 5: Toplinska karta - MAD vs. Ukupan broj transakcija



Prikaz 37: Toplinska karta MAD vrijednosti i Ukupnog broja transakcija za automatizirani sustav

Ova toplinska mapa prikazuje gustoću adresa na temelju kombinacije MAD vrijednosti i ukupnog broja transakcija. Tamnije plave zone označavaju koncentraciju velikog broja adresa, dok svijetle ukazuju na rjeđe kombinacije. Najveća gustoća nalazi se pri niskim MAD vrijednostima i nižem do srednjem broju transakcija, što potvrđuje da većina adresa ne odstupa značajno od Benfordove distribucije i imaju umjerenu aktivnost. Pojedine adrese s visokim MAD-om i visokim brojem transakcija (gornji desni kut) potencijalno upućuju na skriptirano ili automatizirano ponašanje, što može zahtijevati dodatnu analizu.

3.8.3 Evaluacija rezultata automatizirane analize i usporedba sa stvarnim oznakama računa

U ovom istraživanju korišten je Benfordov zakon za identifikaciju potencijalno sumnjivih Ethereum računa, analizirajući varijablu *value* (vrijednost transakcije u ETH). Na temelju

izračunatog MAD pokazatelja, računi su klasificirani u četiri razine konformnosti: *Strong, Moderate, Weak i Nonconformity.*

Kako su izvorni pragovi iz funkcije *benford()* paketa *benford.analysis* razvijeni prvenstveno za financijske izvještaje i knjigovodstvene podatke, u ovom radu uvedeni su prilagođeni pragovi, osjetljiviji na transakcijske obrasce u kriptovalutama. Prema toj kategorizaciji, računi koji se svrstavaju u skupinu *Nonconformity* klasificirani su kao sumnjivi, dok se ostali smatraju legitimnima.

Na temelju tih kriterija, od ukupno 3.513 analiziranih adresa, njih 919 klasificirano je u kategoriju sumnjivih. To čini 26.16 % ukupnih računa, što je vrlo blizu stvarnoj raspodjeli oznaka u izvornim podacima – gdje je 22.14 % računa označeno kao prevarantsko ($FLAG = 1$) - podatak dobiven u prvoj fazi istraživanja pomoću funkcije *prop.table()*.

Min MAD	Max MAD	Conformity
0	0,006	Close conformity
0,006	0,012	Acceptable conformity
0,012	0,015	Marginal conformity
0,015	1	Nonconformity

Tablica 6: Pragovi koje je definirao dr. Mark J. Nigrini, stručnjak za forenzičko računovodstvo i analizu prevara (podrazumijevani u paketu benford.analysis())

Column1	Column2	Column3
0	0,06	Strong conformity
0,06	0,1	Moderate conformity
0,1	0,14	Weak conformity
0,14	1	Nonconformity

Tablica 7: Pragovi ručno prilagođeni za analizu kriptovaluta

Broj računa označenih kao sumnjivi pomoću prilagođenih pragova je približno jednak stvarnom broju prevarnih računa u skupu podataka. Ova usklađenost između predikcije temeljene na Benfordovom zakonu i stvarnih oznaka ukazuje na to da bi ova metoda mogla imati potencijal kao preliminarni alat za detekciju sumnjivih računa u kripto sustavima.

4 Zaključak

U ovom radu detaljno je analiziran značaj i metode detekcije prevara unutar blockchain tehnologije, s naglaskom na njenu ulogu u očuvanju kako financijske sigurnosti, tako i etičkih principa koji su temelj ove tehnologije. Kroz analizu različitih vrsta prevara, uključujući manipulacije u pametnim ugovorima, napade na decentralizirane financijske platforme te lažne NFT projekte, jasno je da blockchain, iako decentraliziran i transparentan, nije imun na zloupotrebe.

Osim analize transakcijskih obrazaca i statističkih pokazatelja, poseban naglasak stavljen je na primjenu Benfordovog zakona kao alata za detekciju anomalija u financijskim podacima. Rezultati su pokazali da odstupanja od predviđene distribucije vodećih znamenki mogu ukazivati na potencijalno sumnjive račune i transakcije. Nadalje, razvijen je automatizirani sustav analize koji kombinira Benfordovu provjeru s ručno prilagođenim pragovima temeljenima na strukturi i ponašanju promatranih računa. Ovakav pristup omogućio je brzu identifikaciju sumnjivih aktivnosti, uz smanjenje broja lažno pozitivnih rezultata.

Razvijeni algoritmi i pristupi za prepoznavanje nepravilnosti u transakcijama i ponašanju korisnika omogućavaju pravovremenu identifikaciju i sprječavanje financijskih gubitaka. Međutim, osim statističke dimenzije, želim naglasiti i etičku važnost ovih sustava – jer bez povjerenja, koje se temelji na sigurnosti i poštenju, blockchain ne može ostvariti svoj puni potencijal kao alat za decentralizaciju i demokratizaciju financija.

Stoga, detekcija prevara predstavlja most između tehničke učinkovitosti i etičke odgovornosti u blockchain okruženju. Kroz sustavnu primjenu ovih metoda, uz inovativne pristupe poput Benfordove analize i adaptivnih pragova, moguće je stvoriti sigurnije i pravednije digitalno okruženje, gdje svi sudionici djeluju unutar okvira transparentnosti i odgovornosti. Ovaj rad potvrđuje kako je kontinuirana inovacija u sigurnosnim praksama neophodna za očuvanje integriteta blockchain sustava, što je ključ za njegovu širu prihvaćenost i dugoročnu održivost.