UDK: 343.359:004.8| DOI:10.5937/etp2601107P
Datum prijema rada: 23.3.2026.
Datum korekcije rada: 2.4.2026.
Datum prihvatanja rada: 10.4.2026.

STRUČNI RAD

EKONOMIJA
TEORIJA I PRAKSA
Godina XIX • broj 1
str. 107–126

ULOGA ALATA VEŠTAČKE INTELIGENCIJE U BORBI PROTIV PRANJA NOVCA I FINANSIRANJA TERORIZMA U SAVREMENOM DIGITALNOM OKRUŽENJU

Petković Aleksandar[1]

Vladisavljević Radovan[2]

Ciganović Petar[3]

Sažetak: *Borba protiv pranja novca i finansiranja terorizma dobija novu dimenziju pojavom digitalnih valuta. Pod digitalne valute spadaju i kriptovalute koje vrlo brzo privlače veliki broj korisnika, uglavnom legitimnih korisnika. Zbog svoje prirode kriptovalute postaju omiljeno sredstvo za pranje novca i finansiranje terorizma (AML/CFT). Same kriptovalute snažno se oslanjaju na pseudoanonimnost kao i na veliku brzinu transakcija. Naime, volumen i brzina transakcija u velikoj meri otežavaju posao agencijama koje su zadužene da se bore protiv pranja novca i finansiranja terorizma. Pojava veštačke inteligencije, kao i specijalizovanih alata bazirani na veštačkoj inteligenciji u velikoj meri pomažu agencijama da brže i tačnije lociraju i transakcije koje se mogu povezati sa pranjem novca i finansiranjem terorizma.*

Ključne reči: *veštačka inteligencija, borba protiv pranja novca i finansiranja novca, kriptovalute, blokčejn.*

[1] Više javno tužilaštvo u Novom Sadu, Sutjeska 2, Novi Sad, tejana.AP@gmail.com, https://orcid.org/0009-0002-0550-7452

[2] Faculty of Economics and Engineering Management in Novi Sad, Cvećarska 2, Novi Sad, radovan.vladisavljevic@fimek.edu.rs, https://orcid.org/0000-0002-8502-8584

[3] Faculty of Economics and Engineering Management in Novi Sad, Cvećarska 2, Novi Sad, pciganovic80@gmail.com, https://orcid.org/0009-0004-4046-1909

UVOD

Terorizam je postao globalna pretnja miru, finansiranje terorizma postaje jedna od ključnih tačaka oko koje su formirane brojne agencije kako nacionalne tako i nadnacionalne. Međutim, pojava kriptovaluta je unela nove izazove u domenu borbe protiv pranja novca i finansiranja terorizma. Kriptovalute se pre svega oslanjaju na pseudo anonimnost, kripto tehnologije i veliku brzinu transakcija. Ovo je dovelo do drastičnog povećanja broja transakcija, kao posledica ovoga je otežana borba protiv pranja novca i finansiranja terorizma.

Pseudoanonimnost se, pre svega, ogleda u tome što se kriptovalute vezuju za digitalne novčanike, a novčanici su vezani za konkretne naloge. Digitalni novčanik je deo elektronskog novca koji je jedna od inovacija u instrumentima plaćanja (Handayani, Novitasari, 2020, 1). Međutim, brzina transakcija kao i različite jurisdikcije onemogućavaju efikasnu borbu protiv pranja novca i finansiranja terorizma. Na to mogu da se dodaju različite tehnologije mešanja kriptovaluta, digitalnih novčanika koji nisu u skladu sa pravilima AML („Anti-Money Laundering" – Sprečavanje pranja novca) i KYC („Know Your Customer" – Upoznajte svog kupca).

U pomoć borbi protiv pranja novca i finansiranja terorizma uskaču alati i tehnike veštačke inteligencije koje mogu pomoći u analizi velikog broja transakcija i označavanje istih kao potencijalno rizične sa stanovišta pranja novca. Kroz rad daće se prikaz alata koji se koriste u domenu AML-a, kao i opis modela koji se koriste u borbi poriv pranja novca. Potrebno je naglasiti i to da su mnogi alati i tehnike vezani za veštačku inteligenciju još uvek u povoju i da rezultati koje ovi alati generišu mogu imati relativno veliki broj lažno pozitivnih pogodaka.

FENOMEN PRANJA NOVCA I TEHNIKE PRANJA NOVCA

Praktično ne postoji jedinstvena definicija pranja novca; umesto toga, postoje brojne definicije koje naglašavaju pojedine aspekte ovog fenomena. Neke definicije, poput one koja se navodi u Varšavskoj konvenciji, glase: „Konverzija ili prenos imovine, uz znanje da ta imovina predstavlja prihod od krivičnog dela, u svrhu sakrivanja ili prikrivanja nezakonitog porekla imovine ili pomaganja bilo kom licu koje je umešano u izvršenje krivičnog dela da izbegne zakonske posledice svojih radnji; sakrivanje ili prikrivanje prave prirode, izvora, lokacije, raspolaganja, kretanja, imovinskih prava ili prava vlasništva nad imovinom, uz znanje

da ta imovina predstavlja prihod stečen od krivičnog dela" (Council of Europe, 2005). Kao što se može videti, ova definicija je vrlo opširna; međutim, druge definicije mogu biti daleko sažetije, poput naredne definicije: „pranje novca označava aktivnosti usmerene ka legalizaciji novca stečenog bavljenjem kriminalnim delatnostima" (Bjelajac, Jovanović, 2012, 101), ili: „pranje novca je proces prikrivanja nezakonitog porekla novca ili imovine stečenih kriminalom" (Uprava za sprečavanje pranja novca, 2011, 3). Definicije uglavnom naglašavaju proces skrivanja porekla novca, odnosno da poreklo novca ne proizilazi iz izvora A, već iz izvora B. Za razliku od pranja novca, finansiranje terorizma ne mora nužno uključivati sredstva nezakonitog porekla; međutim, mehanizmi pranja novca mogu se koristiti radi prikrivanja izvora, kretanja i krajnje namene sredstava namenjenih terorističkim aktivnostima. Finansiranje terorizma je naredni pojam neraskidivo vezan za pranje novca. Terorističke organizacije ugrožavaju kako nacionalne interese, tako mogu ugrožavati i interese međunarodne zajednice. Nasilje je značajno svojstvo terorizma, shvaćeno kao specifična primena sile kojom se namerava, odnosno teži tome, da se suprotna strana dovede u situaciju da se ponaša suprotno svojim namerama i svojoj volji (Stanković, 2014, 10).

Sam proces pranja novca (Sullivan, 2023, 10) najčešće se sastoji od tri faze:

- Faza polaganja („placement"),
- Faza slojevitosti („layering"),
- Faza integracije („integration").

Prva faza pranja novca prema trofaznom modelu jeste faza polaganja (placement), koja podrazumeva ubacivanje nezakonito stečenih sredstava u legalne finansijske tokove. Ova faza se smatra najrizičnijom, jer postoji neposredna vremenska i transakciona blizina između sredstava i njihovog kriminalnog izvora. Osnovna svrha polaganja jeste udaljavanje imovine od njenog nezakonitog porekla i iniciranje procesa njenog daljeg prikrivanja.

U praksi, polaganje može poprimiti različite oblike, uključujući depozite u bankarskom sistemu, ulaganja u nepokretnosti, kupovinu vredne pokretne imovine, korišćenje igara na sreću, kao i investiranje u umetnička dela ili druga dobra visoke vrednosti. Dijapazon mogućih mehanizama je širok i prilagođava se stepenu razvijenosti finansijskog sistema i regulatornog okvira.

Rizik u ovoj fazi proizlazi iz postojanja razvijenih mehanizama za sprečavanje pranja novca (AML – Anti-Money Laundering), koji podrazumevaju obavezu identifikacije klijenata, praćenje transakcija i

prijavljivanje sumnjivih aktivnosti. Veće pojedinačne transakcije, posebno iznosi koji prelaze regulatorno definisane pragove (npr. 10.000 USD u pojedinim jurisdikcijama), automatski aktiviraju kontrolne procedure. Međutim, i veći broj manjih, međusobno povezanih transakcija može izazvati sumnju, što je poznato kao strukturiranje ili „smurfing".

Druga faza pranja novca uključuje mešanje nelegalno stečenih sredstava sa legalno stečenim sredstvima. Pomoću ove faze prekida se trag između nelegalnih sredstava i kriminalnih aktivnosti. Ovde se sve teže uočava razlika između legalno stečenih i nelegalno stečenih sredstava. Tehnike slojevitosti („layering") najčešće uključuju višestruke transfere između različitih računa i banaka, a takođe najčešće prevazilaze nacionalne granice. Ovo je ujedno i razlog za međunarodnu saradnju i formiranje tela koja se bore protiv pranja novca i finansiranja terorizma na internacionalnom nivou. Jedno od važnijih tela je FATF („Financial Action Task Force"), koje, iako jedno od najvažnijih, nije i jedino telo koje se bavi sprečavanjem pranja novca i finansiranjem terorizma na međunarodnom nivou.

Kriptovalute su se pokazale kao relativno dobar način za zametanje traga nelegalno stečenom novcu. Ova relativno nova tehnologija dovoljno je robusna i fleksibilna za potrebe pranja novca i finansiranja terorizma. Kriptovalute se oslanjaju na pseudoanonimnost i veliku brzinu transakcija, a priroda interneta je takva da nacionalne granice nisu velika prepreka za slanje i primanje digitalnih signala. Decentralizovana priroda kriptovaluta pruža dodatni nivo zaštite u domenu pranja novca i finansiranja terorizma. Odnosno, ne postoji centralni autoritet koji bi mogao pratiti transakcije kriptovaluta.

Poslednja faza ovog modela pranja novca i finansiranja terorizma jeste integracija („integration") nelegalnog novca sa legalnim tokovima novca. Na ovaj način nelegalno stečena sredstva gube svoj trag porekla i u ovoj fazi je veoma teško razlikovati legalna od ilegalnih sredstava. Sredstva stečena kriminalnim aktivnostima praktično postaju legalna sredstva. Međutim, kod finansiranja terorizma cilj najčešće nije zametanje nelegalnih izvora sredstava, već zaštita izvora finansiranja.

Premisa kod finansiranja terorizma je da se terorističke organizacije često finansiraju od dobrovoljnih priloga ili od strane pojedinaca ili grupacija koje podržavaju ove organizacije. U velikom broju slučajeva finansiranje terorizma nije legalna radnja i podleže sankcijama. Baš iz ovog razloga izvori finansiranja terorizma se skrivaju. Kod finansiranja terorizma sredstva ne moraju biti nezakonitog porekla, ali je često ključno prikriti tok i krajnju namenu sredstava, a ne samo njihov izvor.

Hamas je u više navrata koristio javne kripto-adrese (najčešće Bitcoin) za prikupljanje donacija putem interneta. Te adrese su bile objavljivane na njihovim sajtovima ili povezanim kanalima i svako je mogao da pošalje sredstva. Zbog transparentnosti blockchaina, javne adrese su paradoksalno lakše za praćenje nego tradicionalni gotovinski tokovi. Upravo zato su mnoge ekstremističke i sankcionisane grupe kasnije prešle na neke alternativne načine finansiranja. Često se radi o kraćim akcijama finansiranja, upotrebi posrednika ili češćem menjanju adresa za prikupljanje sredstava.

Iako se tradicionalni model pranja novca zasniva na trofaznoj strukturi, savremeni oblici u digitalnom okruženju ukazuju na postojanje dodatne operativne faze redistribucije ili „izvlačenja" sredstava, koja podrazumeva njihovu finalnu konverziju i stavljanje pod direktnu kontrolu krajnjeg korisnika. Odnosno, kriptovalute se u jednom momentu moraju pretvoriti u neku važeću novčanu valutu. Ovo je naročito važno za terorističke organizacije, jer je gotovinu daleko teže pratiti nego digitalne valute.

MEĐUNARODNA TELA ZA BORBU PROTIV PRANJA NOVCA I FINANSIRANJA TERORIZMA

Fenomen pranja novca i finansiranja terorizma predstavlja izuzetno ozbiljnu pretnju svetskom miru, te su formirana brojna tela koja se bave borbom protiv ovog fenomena. Praktično, svaka država sveta pokušava da se izbori sa nezakonitim delovanjima, naročito u domenu organizovanog kriminala, koji može u velikoj meri da izazove brojne negativne posledice kako za sigurnost i zdravlje građana jedne države, tako i za ekonomsku, ali i političku stabilnost celokupnog društva. Iz ovog razloga formirana su brojna međunarodna i nacionalna tela, a u narednoj tabeli data su samo neka od važnijih međunarodnih tela za borbu protiv pranja novca i finansiranja terorizma. Koliko je ova tema značajna, može se videti na primeru preporuka FATF-a, koje se od 36. do 40. preporuke odnose na formiranje međunarodne saradnje u domenu borbe protiv pranja novca i finansiranja terorizma (AML Expert, 2016, 221).

Tabela 1. Međunarodne institucije koje se bave borbom protiv pranja novca i finansiranja terorizma

Institucija	Tip tela	Primarna funkcija	Nivo delovanja	Veza sa AML/CFT sistemom
Financial Action Task Force (FATF)	Globalni standardi	Donosi međunarodne standarde (40 preporuka)	Globalni	Postavlja normativni okvir za AML/CFT
MONEYVAL	Regionalno evaluaciono telo	Procena usklađenosti država sa FATF standardima	Regionalni (Savet Evrope)	Nadzor implementacije
Egmont Group	Operativna mreža	Razmena informacija između FIU	Globalni	Operativna saradnja u istragama
Basel Committee on Banking Supervision	Regulatorno telo	Standardi bankarskog nadzora i upravljanja rizicima	Globalni	Indirektno jača AML kroz prudencijalni nadzor
International Monetary Fund (MMF)	Finansijska institucija	Procena finansijskih sistema, tehnička pomoć	Globalni	AML/CFT kao deo finansijske stabilnosti
United Nations Office on Drugs and Crime	UN agencija	Razvoj konvencija i tehnička podrška	Globalni	Normativni i razvojni okvir borbe protiv kriminala

Izvor: Autori

Tabela 2. Infrastruktura Bitcoin i Monero kriptovalute

Element	Bitcoin	Monero
Pošiljalac	Javan (adresa)	Sakriven (ring signature)
Primalac	Javan (adresa)	Sakriven (stealth adresa)
Iznos	Javan	Sakriven
Forenzička analiza	Vrlo razvijena	Izuzetno otežana

Izvor: Autori

Međunarodna arhitektura za borbu protiv pranja novca i finansiranja terorizma ne predstavlja centralizovan i hijerarhijski organizovan sistem, već višeslojnu mrežu institucionalno povezanih i funkcionalno komplementarnih aktera. Ovu mrežu čine normativna tela koja postavljaju globalne standarde, evaluacioni mehanizmi koji procenjuju njihovu primenu, operativne strukture zadužene za razmenu informacija i finansijske institucije koje integrišu ove standarde u sistem finansijskog nadzora i stabilnosti. Takva struktura omogućava istovremeno oblikovanje međunarodnih pravila, nadzor nad njihovom implementacijom i praktičnu saradnju u konkretnim slučajevima.

Normativni nivo sistema usmeren je na definisanje univerzalnih principa i preporuka koje države inkorporiraju u svoja zakonodavstva. Time se obezbeđuje određeni stepen harmonizacije pravnih i regulatornih okvira, što je od ključne važnosti u uslovima globalizovanih finansijskih tokova. Evaluacioni mehanizmi doprinose kredibilitetu sistema kroz periodične procene usklađenosti nacionalnih sistema sa međunarodnim standardima, čime se podstiče kontinuirano unapređenje zakonodavstva i institucionalnih kapaciteta. Operativni nivo, zasnovan na saradnji nacionalnih nadležnih organa, omogućava razmenu podataka i koordinaciju istraga, čime se prevazilaze ograničenja nacionalnih jurisdikcija.

Posebnu dimenziju ove arhitekture čini njena povezanost sa širim konceptom globalnog upravljanja finansijskim rizicima. Sprečavanje pranja novca i finansiranja terorizma posmatra se ne samo kao bezbednosno pitanje već i kao pitanje očuvanja integriteta i stabilnosti finansijskog sistema. Zbog toga su u sistem uključene i međunarodne finansijske institucije koje kroz nadzor, tehničku pomoć i uslovljavanje finansijske podrške utiču na jačanje nacionalnih kapaciteta.

U celini posmatrano, globalni AML/CFT sistem funkcioniše kao mrežni model upravljanja zasnovan na standardizaciji, evaluaciji i međunarodnoj saradnji. Njegova efikasnost ne proizlazi iz centralizovane kontrole, već iz međusobne povezanosti aktera i reputacionog pritiska koji podstiče države da usklađuju svoje sisteme sa međunarodnim normama. Ovakav model predstavlja primer savremenog globalnog upravljanja u oblasti finansijske bezbednosti, gde su normativni, regulatorni i operativni elementi objedinjeni u jedinstven, ali decentralizovan sistem.

Ovo je na međunarodnom nivou, dok na nacionalnom nivou borba protiv pranja novca i finansiranja terorizma funkcioniše kroz tri nivoa:

- preventivni nivo (obveznici i nadzorni organi),
- analitički nivo (Finansijsko-obaveštajna jedinica, FIU; u Republici Srbiji to telo nosi naziv: Uprava za sprečavanje pranja novca),
- represivni nivo (policija, tužilaštvo, sudovi).

Nacionalna struktura za sprečavanje pranja novca i finansiranja terorizma u Republici Srbiji zasniva se na integrisanom sistemu preventivnih, analitičkih i represivnih mehanizama, koji funkcionišu u međusobnoj koordinaciji i u skladu sa međunarodnim standardima. Ovaj sistem ima za cilj zaštitu integriteta finansijskog poretka, sprečavanje zloupotrebe finansijskih tokova i jačanje institucionalne otpornosti na finansijski kriminal.

Pravni temelj sistema čini zakonodavni okvir kojim se uređuju obaveze obveznika, mere dubinske analize stranaka, prijavljivanje sumnjivih aktivnosti i postupanje nadležnih organa. U okviru analitičkog segmenta centralnu ulogu ima finansijsko-obaveštajna jedinica, koja prikuplja, obrađuje i analizira podatke o sumnjivim transakcijama i, po potrebi, dostavlja ih nadležnim organima na dalje postupanje. Ova institucija predstavlja ključnu tačku povezivanja između finansijskog sektora i organa krivičnog gonjenja.

Preventivna dimenzija sistema ostvaruje se kroz nadzor nad finansijskim i nefinansijskim obveznicima, pri čemu regulatorna tela kontrolišu primenu propisanih mera identifikacije klijenata, procene rizika i unutrašnjih kontrola. Time se nastoji da se potencijalne zloupotrebe identifikuju u ranoj fazi i spreči ulazak nezakonitih sredstava u legalne tokove. Represivni segment sistema obuhvata policijske organe, tužilaštvo i sudove, koji postupaju u slučajevima kada postoje osnovi sumnje da je izvršeno krivično delo pranja novca ili finansiranja terorizma.

Posebnu važnost ima međuinstitucionalna saradnja, kao i strateško planiranje zasnovano na nacionalnoj proceni rizika, koja omogućava usmeravanje resursa ka sektorima i aktivnostima sa povećanim stepenom izloženosti. U uslovima digitalizacije finansijskog sektora i razvoja novih oblika imovine, nacionalni sistem se kontinuirano prilagođava kako bi obuhvatio i nove učesnike na tržištu, čime se dodatno jača sveobuhvatnost i efikasnost mehanizama za zaštitu finansijskog sistema.

DARK WEB I MIKSERI NOVCA

Dark web predstavlja deo interneta koji nije indeksiran standardnim pretraživačima i kojem se pristupa putem specijalizovanih alata i mreža za anonimnu komunikaciju. Najpoznatiji sistem za pristup dark web sadržajima je Tor (The Onion Router), koji omogućava višeslojno šifrovanje i usmeravanje internet saobraćaja kroz niz distribuiranih čvorova, čime se otežava identifikacija korisnika i lokacije servera.

Važno je razlikovati tri pojma koji se često pogrešno izjednačavaju: surface web, deep web i dark web. Surface web čini javno dostupan i indeksiran deo interneta. Deep web obuhvata sav sadržaj koji nije indeksiran (npr. baze podataka, akademski portali, privatni sistemi). Dark web je specifičan podskup deep weba koji zahteva posebne protokole i alate za pristup i koji je dizajniran sa naglašenim fokusom na anonimnost.

U javnosti se dark web često poistovećuje isključivo sa kriminalnim aktivnostima, ali takvo shvatanje je pojednostavljeno i netačno. Iako na dark webu zaista postoje platforme koje su povezane sa nezakonitim trgovinama, sajber-kriminalom ili distribucijom zabranjenog sadržaja, značajan deo tog prostora koristi se u legitimne svrhe. Na primer, novinari, istraživači i uzbunjivači koriste anonimne mreže radi zaštite identiteta i komunikacije sa poverljivim izvorima. Organizacije za zaštitu ljudskih prava, politički aktivisti u represivnim režimima, kao i građani u zemljama sa cenzurom interneta, koriste dark web kao sredstvo očuvanja slobode izražavanja i pristupa informacijama.

Pojedini mediji i međunarodne organizacije omogućavaju bezbedne kanale za dostavljanje informacija upravo putem anonimnih mreža poput Tora. Time dark web postaje instrument zaštite privatnosti i digitalnih prava, a ne nužno prostor kriminala. Sama tehnologija anonimnosti je neutralna; njen karakter zavisi od načina upotrebe. Tor (The Onion Router) je decentralizovana mreža dizajnirana da omogući anonimnu komunikaciju na internetu. Nastala je sa ciljem zaštite privatnosti korisnika i onemogućavanja praćenja internet saobraćaja, kako od strane komercijalnih aktera, tako i od strane državnih nadzornih sistema. Tor funkcioniše na principu višeslojnog šifrovanja i rutiranja podataka kroz niz distribuiranih čvorova širom sveta.

Osnovni princip rada Tor mreže zasniva se na takozvanom „onion routing" modelu. Kada korisnik pristupa internetu putem Tora, njegov saobraćaj se ne šalje direktno ka odredišnom serveru. Umesto toga, podaci prolaze kroz najmanje tri nasumično izabrana čvora: ulazni (entry node), srednji

(relay node) i izlazni (exit node). Svaki sloj prenosa je dodatno šifrovan, slično slojevima luka, zbog čega se koristi termin „onion". Svaki čvor zna samo od koga je primio podatke i kome ih dalje prosleđuje, ali ne i kompletnu putanju ili krajnji izvor i destinaciju. Na taj način se značajno otežava identifikacija korisnika.

Tor mreža omogućava pristup standardnim internet stranicama, ali i specifičnim servisima sa .onion domenom, koji su dostupni isključivo unutar same mreže. Ovi servisi dodatno štite identitet servera, jer ni njihova fizička lokacija nije javno dostupna. Time se obezbeđuje dvosmerna anonimnost — i korisnika i pružaoca usluge.

Primena Tor mreže je višestruka. Koriste je novinari, istraživači i organizacije za ljudska prava radi zaštite komunikacije i izvora informacija. U zemljama sa cenzurom interneta Tor predstavlja sredstvo zaobilaženja blokada i pristupa informacijama. Takođe, pojedine institucije omogućavaju bezbedne kanale za dostavljanje poverljivih dokumenata putem Tor infrastrukture.

Istovremeno, zbog visokog nivoa anonimnosti, Tor može biti zloupotrebljen za nezakonite aktivnosti. Međutim, sama tehnologija je neutralna; ona pruža alat za zaštitu privatnosti, dok način upotrebe zavisi od korisnika. Upravo zbog toga Tor mreža zauzima specifično mesto u savremenim raspravama o digitalnoj bezbednosti, privatnosti i regulaciji interneta.

Sa stanovišta bezbednosnih i regulatornih analiza, Tor predstavlja izazov jer otežava identifikaciju IP adresa i praćenje komunikacije. Ipak, on istovremeno predstavlja važan instrument zaštite osnovnih digitalnih prava, naročito u kontekstu slobode izražavanja i zaštite privatnosti u savremenom informacionom društvu. Razumevanjem prepreka sajber-bezbednosti koje nastaju zbog količine, brzine i raznolikosti podataka, lako je shvatiti napore koje ove oblasti zahtevaju (Jhanjhi, 2025, 200).

Sa aspekta bezbednosti i regulacije, dark web predstavlja izazov jer otežava identifikaciju učesnika u komunikaciji i finansijskim transakcijama, naročito kada se kombinuje sa kriptovalutama. Međutim, pogrešno bi bilo smatrati da je čitav dark web inherentno kriminalan. On je tehnološki prostor sa dvostrukom prirodom: može služiti i legitimnim ciljevima zaštite privatnosti i nezakonitim aktivnostima. Zbog toga se u savremenim analizama sve više naglašava potreba za diferenciranim pristupom — fokusom na suzbijanje konkretnih kriminalnih aktivnosti, uz istovremeno očuvanje legitimnih prava na anonimnost i slobodu komunikacije.

Mikseri kriptovaluta (poznati i kao „tumblers") predstavljaju specijalizovane servise ili protokole čija je osnovna funkcija prekidanje veze između adrese pošiljaoca i adrese primaoca u okviru blockchain transakcija. Njihova svrha je povećanje privatnosti korisnika tako što otežavaju ili onemogućavaju praćenje toka sredstava putem javne blockchain analitike.

U sistemima poput Bitcoina, gde su sve transakcije javno vidljive, moguće je pratiti tok sredstava kroz niz adresa i rekonstruisati obrasce kretanja kapitala. Iako su adrese pseudonimne, napredne forenzičke metode omogućavaju povezivanje transakcija i identifikaciju korisnika, naročito kada se koristi regulisana berza sa KYC procedurama. Mikseri su razvijeni kao odgovor na ovu transparentnost.

Osnovni princip rada miksera zasniva se na „mešanju" sredstava više korisnika. Korisnik šalje određenu količinu kriptovalute na adresu miksera, a nakon određenog vremena prima ekvivalentan iznos (umanjen za proviziju) sa druge adrese koja nije direktno povezana sa prvobitnom uplatom. U međuvremenu, sredstva se kombinuju sa sredstvima drugih korisnika, čime se prekida jasan trag između ulazne i izlazne transakcije. Cilj je stvaranje složenog i teško rekonstruisivog transakcionog lanca.

Postoje dva osnovna modela miksera. Prvi su centralizovani servisi, gde treća strana upravlja procesom mešanja i privremeno preuzima kontrolu nad sredstvima. Ovaj model podrazumeva visok nivo poverenja u operatera servisa, ali i rizik od prevara ili zaplene sredstava. Drugi model su decentralizovani protokoli, koji funkcionišu putem pametnih ugovora na mrežama kao što je Ethereum. U tim slučajevima proces mešanja se automatizuje kroz kriptografske mehanizme, bez centralnog posrednika.

Sa stanovišta legitimne upotrebe, mikseri mogu biti sredstvo zaštite finansijske privatnosti korisnika koji ne žele da njihova istorija transakcija bude javno dostupna. U određenim okolnostima, naročito u zemljama sa visokim nivoom nadzora ili političke represije, ovakvi alati mogu imati funkciju zaštite osnovnih prava na privatnost.

Međutim, sa regulatornog i bezbednosnog aspekta, mikseri predstavljaju značajan izazov. Zbog sposobnosti da prikriju poreklo sredstava, često se povezuju sa fazom „layering" u procesu pranja novca, gde je cilj otežavanje praćenja nezakonito stečenog kapitala. Takođe se mogu koristiti za prikrivanje tragova finansiranja nezakonitih aktivnosti. Upravo zbog toga su pojedini mikseri i njihovi operateri bili predmet sankcija i istraga u više država.

U savremenom digitalnom finansijskom okruženju mikseri ilustruju širu dilemu između prava na finansijsku privatnost i potrebe za efikasnom primenom AML/CFT mehanizama. Tehnološki gledano, oni predstavljaju alat za povećanje anonimnosti u transparentnim blockchain sistemima; regulatorno gledano, oni su potencijalni instrument za prikrivanje nezakonitih tokova kapitala.

TEHNIKE BORBE PROTIV PRANJA NOVCA I FINANSIRANJA TERORIZMA

Borba protiv pranja novca i finansiranja terorizma zasniva se na kombinaciji regulatornih, institucionalnih i tehnoloških mehanizama čiji je cilj identifikacija, praćenje i sprečavanje nezakonitih tokova kapitala. Savremeni pristup AML/CFT sistemima polazi od pretpostavke da finansijski sektor predstavlja ključnu tačku kontrole, jer gotovo svaka značajnija finansijska aktivnost u nekom trenutku dolazi u dodir sa bankama, platnim institucijama, investicionim fondovima ili drugim finansijskim posrednicima. Zbog toga su upravo te institucije obavezane da primenjuju preventivne i detekcione mehanizme.

Jedna od centralnih tehnika u borbi protiv pranja novca jeste princip „Know Your Customer" (KYC), odnosno upoznavanje klijenta. Suština KYC-a je da finansijska institucija mora pouzdano da utvrdi identitet klijenta pre uspostavljanja poslovnog odnosa, ali i tokom njegovog trajanja. To podrazumeva prikupljanje identifikacionih podataka, proveru autentičnosti dokumenata, utvrđivanje stvarnog vlasnika pravnog lica, kao i razumevanje prirode i svrhe poslovnog odnosa. KYC nije jednokratan čin, već kontinuirani proces koji uključuje praćenje promena u ponašanju klijenta i ažuriranje podataka.

KYC se nadovezuje na širi koncept dubinske analize klijenta (Customer Due Diligence – CDD). Ovaj pristup podrazumeva procenu rizika koji određeni klijent, transakcija ili poslovni odnos mogu predstavljati. U zavisnosti od procenjenog nivoa rizika, primenjuju se različiti nivoi kontrole. Kod klijenata sa povišenim rizikom, kao što su politički eksponirana lica (PEP), primenjuje se pojačana dubinska analiza (Enhanced Due Diligence – EDD), koja uključuje detaljnije provere porekla sredstava i intenzivnije praćenje transakcija. Ovakav pristup zasniva se na principu upravljanja rizikom, gde se resursi usmeravaju na one oblasti u kojima postoji veća verovatnoća zloupotrebe.

Druga važna tehnika jeste kontinuirani monitoring transakcija. Finansijske institucije koriste sofisticirane softverske sisteme koji

analiziraju obrasce ponašanja i prepoznaju neuobičajene ili sumnjive aktivnosti. To može uključivati nagle promene u obimu transakcija, učestale transfere prema jurisdikcijama visokog rizika ili razbijanje velikih iznosa na više manjih transakcija. Kada se identifikuje sumnjiva aktivnost, institucija je dužna da podnese izveštaj nadležnoj finansijsko-obaveštajnoj jedinici (FIU), čime se aktivira dalji institucionalni mehanizam provere.

Značajnu ulogu ima i koncept stvarnog vlasništva (beneficial ownership), čiji je cilj da se otkrije fizičko lice koje ima krajnju kontrolu nad pravnim subjektom ili sredstvima. U praksi se pranje novca često oslanja na složene korporativne strukture, ofšor kompanije i posrednike kako bi se prikrio identitet stvarnog vlasnika. Transparentnost vlasničkih struktura predstavlja zato ključni element efikasne prevencije.

U digitalnom okruženju, naročito u oblasti kriptovaluta i finansijskih tehnologija, razvijaju se dodatni mehanizmi poput e-KYC procedura, biometrijske identifikacije i primene veštačke inteligencije u analizi podataka. Ovi sistemi omogućavaju bržu i precizniju procenu rizika, ali istovremeno otvaraju pitanja zaštite podataka i privatnosti. Balans između efikasnog nadzora i očuvanja osnovnih prava postaje centralno pitanje savremenih AML/CFT politika.

Borba protiv pranja novca i finansiranja terorizma danas se ne zasniva samo na represivnim merama, već pre svega na preventivnim tehnikama koje imaju za cilj da otežaju ulazak nezakonitog kapitala u legalne finansijske tokove. KYC i srodni mehanizmi predstavljaju temelj tog sistema, jer omogućavaju identifikaciju učesnika, razumevanje njihovog finansijskog ponašanja i pravovremeno reagovanje na rizike. Upravo kroz kombinaciju identifikacije, procene rizika, praćenja i institucionalne saradnje stvara se integrisani okvir zaštite finansijskog sistema od zloupotreba.

ALATI VEŠTAČKE INTELIGENCIJE

Primena veštačke inteligencije u borbi protiv pranja novca (AML) i finansiranja terorizma (CFT) u oblasti kriptovaluta zasniva se na sposobnosti algoritama da analiziraju ogromne količine transakcionih podataka, prepoznaju obrasce i identifikuju anomalije koje bi ljudskom analizom ostale neprimećene. S obzirom na javnu prirodu većine blockchain mreža, kriptovalute su istovremeno izazov i prilika za primenu naprednih analitičkih tehnika. Praćenje transakcija u svrhu sprečavanja

pranja novca, u svojoj suštini, predstavlja industrijsku primenu prognoziranja. Prognoziranje je oblast analitike u kojoj se podaci koriste za podešavanje i treniranje modela radi optimizacije izlaza ovih modela u smislu željenog krajnjeg rezultata (Chau, 2021, 27).

Jedan od najvažnijih AI alata u ovoj oblasti jeste analiza transakcionih grafova (graph analytics). Blockchain se može posmatrati kao velika mreža čvorova (adresa) i veza (transakcija). Primena algoritama mašinskog učenja omogućava identifikaciju klastera adresa koje verovatno pripadaju istom subjektu, kao i prepoznavanje tipičnih obrazaca ponašanja povezanih sa fazama pranja novca, naročito fazom „layering". Mašinsko učenje (ML) jedna je od aplikacija veštačke inteligencije (AI) koja ima za cilj da obuči mašinu koristeći istorijske podatke (Alkhalili et al., 2021, 18484). Ovi sistemi koriste tehnike poput detekcije zajednica (community detection), centralnosti čvorova i analize tokova kapitala kako bi rekonstruisali složene finansijske mreže.

Druga značajna primena odnosi se na detekciju anomalija. Modeli nadgledanog i nenadgledanog učenja analiziraju istorijske podatke i formiraju „normalan" obrazac ponašanja određene adrese ili grupe korisnika. Kada se pojavi odstupanje — nagla promena volumena transakcija, neobična interakcija sa visokorizičnim adresama ili transfer ka jurisdikcijama pod sankcijama — sistem generiše upozorenje. Ovakvi modeli su posebno korisni u realnom vremenu, jer omogućavaju brzu reakciju pre nego što se sredstva dalje disperzuju.

U praksi se koriste i modeli za procenu rizika adresa i novčanika (risk scoring). AI sistemi kombinuju podatke o prethodnim vezama sa poznatim nelegalnim aktivnostima, učestalosti transakcija, vrsti korišćenih servisa (npr. miksera) i geografskoj izloženosti. Na osnovu tih parametara generiše se numerički indeks rizika koji pomaže finansijskim institucijama i berzama da odluče da li je potrebna dodatna dubinska analiza.

Poseban segment odnosi se na praćenje tokova kroz decentralizovane finansije (DeFi). S obzirom na složenost pametnih ugovora na mrežama poput Ethereuma, AI alati analiziraju interakcije između protokola, likvidnosnih bazena i cross-chain mostova. Cilj je identifikacija pokušaja prikrivanja porekla sredstava kroz više slojeva decentralizovanih aplikacija.

U oblasti kriptovaluta razvijene su i specijalizovane platforme koje integrišu AI i blockchain forenziku. Među poznatijim kompanijama su Chainalysis, Elliptic i TRM Labs. Ove platforme koriste mašinsko učenje za

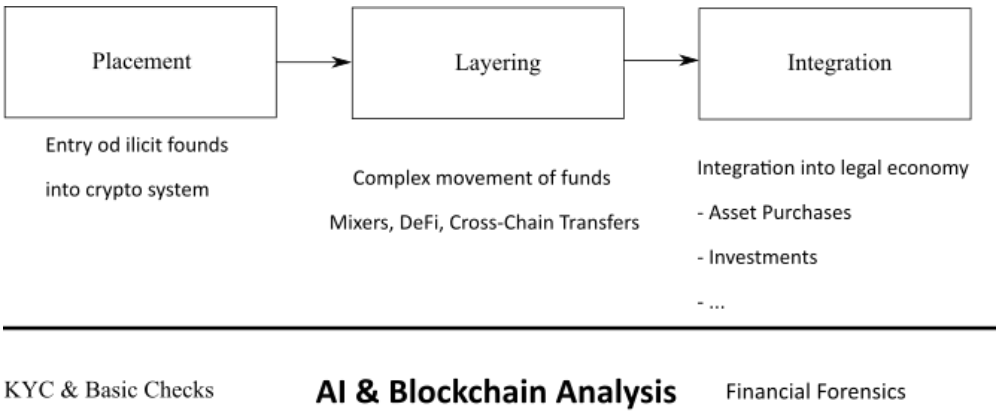
klasifikaciju adresa, identifikaciju povezanosti sa nezakonitim tržištima i generisanje izveštaja za regulatorne organe i finansijske institucije.

Veštačka inteligencija se takođe primenjuje u analizi otvorenih izvora podataka (OSINT), gde se kombinuju blockchain podaci sa informacijama sa društvenih mreža, foruma i dark web platformi. Korišćenjem obrade prirodnog jezika (NLP) moguće je identifikovati obrasce komunikacije i potencijalne veze između digitalnih identiteta i kripto-adresa.

Ipak, važno je naglasiti da AI alati nisu nepogrešivi. Postoji rizik od lažno pozitivnih rezultata, kao i mogućnost da sofisticirani akteri prilagode svoje ponašanje kako bi izbegli detekciju. Pored toga, primena AI u ovoj oblasti otvara pitanja transparentnosti algoritama, zaštite podataka i proporcionalnosti nadzora. Nažalost, AI je još uvek nova tehnologija koja nije dovoljno istražena i koja ima dosta nepoznatih detalja.

U kontekstu kriptovaluta, veštačka inteligencija predstavlja ključni instrument savremenih AML/CFT strategija jer omogućava analizu globalnih, decentralizovanih i visokodinamičnih finansijskih tokova. Kombinacijom graf-analitike, detekcije anomalija, procene rizika i analize podataka iz više izvora, AI sistemi značajno unapređuju sposobnost identifikacije i prevencije zloupotreba u digitalnom finansijskom prostoru.

Model upotrebe veštačke inteligencije u borbi protiv pranja novca i finansiranja terorizma.



Slika 1. Model

Ako uzmemo u obzir klasični model pranja novca, može se reći da je upotreba AI najefikasnija u domenu uslojavanja novca, odnosno mešanja novca sa legitimnim sredstvima kako bi se izgubio trag nezakonito stečenim sredstvima. Ubacivanje novca u legalne sisteme prvi je korak u ovom modelu, a ujedno je ovaj segment i jedan od najranjivijih. U početnom segmentu nezakonita sredstva mogu se najlakše identifikovati; upravo je ovo mesto gde su razvijeni i implementirani relativno sofisticirani modeli borbe protiv pranja novca i finansiranja terorizma. U svetu kriptovaluta ubacivanje sredstava je dosta netransparentno jer postoje različite menjačnice kriptovaluta koje rade pod različitim jurisdikcijama.

Kod poslednjeg segmenta, integracije, veoma je teško razdvojiti sredstva koja su stečena na nezakonit način od legalno stečenih sredstava. Ovde se mora pristupiti relativno kompleksnim modelima forenzičke analize. Sredstva u ovom segmentu modela vrlo često prelaze u neki drugi oblik i definitivno im se gubi trag. U svetu kriptovaluta moguća je pojava otežanog transfera kriptovaluta u fiat valute, kao i transfera fiat valuta iz jedne jurisdikcije u drugu.

Srednji segment modela vezanog za pranje novca i finansiranje terorizma odnosi se na mešanje sredstava. Upravo je ovo segment u kojem veštačka inteligencija ima najviše efekata. Alati veštačke inteligencije relativno brzo mogu analizirati blokove u lancu, tako da mogu pratiti trag transfera kriptovaluta.

ZAKLJUČAK

Primena veštačke inteligencije u borbi protiv pranja novca (AML) i finansiranja terorizma (CFT) u oblasti kriptovaluta zasniva se na sposobnosti algoritama da analiziraju ogromne količine transakcionih podataka, prepoznaju obrasce i identifikuju anomalije koje bi ljudskom analizom ostale neprimećene. S obzirom na javnu prirodu većine blockchain mreža, kriptovalute su istovremeno izazov i prilika za primenu naprednih analitičkih tehnika.

Jedan od najvažnijih AI alata u ovoj oblasti jeste analiza transakcionih grafova (graph analytics). Blockchain se može posmatrati kao velika mreža čvorova (adresa) i veza (transakcija). Primena algoritama mašinskog učenja omogućava identifikaciju klastera adresa koje verovatno pripadaju istom subjektu, kao i prepoznavanje tipičnih obrazaca ponašanja povezanih sa fazama pranja novca, naročito fazom „layering". Ovi sistemi koriste tehnike poput detekcije zajednica

(community detection), centralnosti čvorova i analize tokova kapitala kako bi rekonstruisali složene finansijske mreže.

Druga značajna primena odnosi se na detekciju anomalija. Modeli nadgledanog i nenadgledanog učenja analiziraju istorijske podatke i formiraju „normalan" obrazac ponašanja određene adrese ili grupe korisnika. Kada se pojavi odstupanje — nagla promena volumena transakcija, neobična interakcija sa visokorizičnim adresama ili transfer ka jurisdikcijama pod sankcijama — sistem generiše upozorenje. Ovakvi modeli su posebno korisni u realnom vremenu, jer omogućavaju brzu reakciju pre nego što se sredstva dalje disperzuju.

U praksi se koriste i modeli za procenu rizika adresa i novčanika (risk scoring). AI sistemi kombinuju podatke o prethodnim vezama sa poznatim nelegalnim aktivnostima, učestalosti transakcija, vrsti korišćenih servisa (npr. miksera) i geografskoj izloženosti. Na osnovu tih parametara generiše se numerički indeks rizika koji pomaže finansijskim institucijama i berzama da odluče da li je potrebna dodatna dubinska analiza.

Poseban segment odnosi se na praćenje tokova kroz decentralizovane finansije (DeFi). S obzirom na složenost pametnih ugovora na mrežama poput Ethereuma, AI alati analiziraju interakcije između protokola, likvidnosnih bazena i cross-chain mostova. Cilj je identifikacija pokušaja prikrivanja porekla sredstava kroz više slojeva decentralizovanih aplikacija.

U oblasti kriptovaluta razvijene su i specijalizovane platforme koje integrišu AI i blockchain forenziku. Među poznatijim kompanijama su Chainalysis, Elliptic i TRM Labs. Ove platforme koriste mašinsko učenje za klasifikaciju adresa, identifikaciju povezanosti sa nezakonitim tržištima i generisanje izveštaja za regulatorne organe i finansijske institucije.

Veštačka inteligencija se takođe primenjuje u analizi otvorenih izvora podataka (OSINT), gde se kombinuju blockchain podaci sa informacijama sa društvenih mreža, foruma i dark web platformi. Korišćenjem obrade prirodnog jezika (NLP) moguće je identifikovati obrasce komunikacije i potencijalne veze između digitalnih identiteta i kripto-adresa.

Ipak, važno je naglasiti da AI alati nisu nepogrešivi. Postoji rizik od lažno pozitivnih rezultata, kao i mogućnost da sofisticirani akteri prilagode svoje ponašanje kako bi izbegli detekciju. Pored toga, primena AI u ovoj oblasti otvara pitanja transparentnosti algoritama, zaštite podataka i proporcionalnosti nadzora.

U kontekstu kriptovaluta, veštačka inteligencija predstavlja ključni instrument savremenih AML/CFT strategija jer omogućava analizu

globalnih, decentralizovanih i visokodinamičnih finansijskih tokova. Kombinacijom graf-analitike, detekcije anomalija, procene rizika i analize podataka iz više izvora, AI sistemi značajno unapređuju sposobnost identifikacije i prevencije zloupotreba u digitalnom finansijskom prostoru.

LITERATURA

1. Bjelajac, Đ., Ž., Jovanović, B., M. (2012). Specifičnosti fenomena pranja novca, u *Kultura polisa,* Serbia, 9 (3), 99-118.
2. Uprava za sprečavanje pranja novca. (2011). *Tipologije pranja novca u Republici Srbiji*. Beograd: Uprava za sprečavanje pranja novca. Dostupno na https://www.apml.gov.rs/uploads/useruploads/Documents/977_tipologije-pranja-novca-u-republici-srbiji-13-09-2011.pdf
3. Council of Europe (2005) *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)*, Warsaw, 16 May. Dostupno na: https://rm.coe.int/09000016808eaa5a
4. Stanković, N. (2014). *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko.
5. Sullivan, K. (2023) *Anti-money laundering in a nutshell: Awareness and compliance for financial personnel and business managers*. Berkeley, CA, Berkeley, CA: Apress Apress.
6. Chainalysis (2023, January 12). 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking. Chainalysis. Available at: https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/
7. Sabry, F., Labda, W., Erbad, A., & Malluhi, Q. (2020). Cryptocurrencies and artificial intelligence: Challenges and opportunities. *IEEe Access*, *8*, 175840-175858. https://doi.org/10.1109/ACCESS.2020.3025211
8. Handayani, T., & Novitasari, A. (2020). Digital Wallet as a Transaction Media in The Community. IOP Conference Series: *Materials Science and Engineering,* 879, 012001. https://doi.org/10.1088/1757-899x/879/1/012001
9. Hileman, G., & Rauchs, M. (2017). *Global Cryptocurrencies Benchmarking Study.* Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School.

10. Zohuri, B., Nguyen, H. T., & Moghaddam, M. (2022). What is the Cryptocurrency. Is it a threat to our national security, Domestically and Globally?, *International Journal of Theoretical & Computational Physics*, 3 (1), 1-14.
11. Rizky, A., Lutfiani, N., Mariyati, W., Sari, A., & Febrianto, K. (2022). Decentralization of information using blockchain technology on mobile apps e-journal. *Blockchain Frontier Technology*, 1(2), 1-10. https://doi.org/10.34306/bfront.v1i2.37
12. Jhanjhi, Z., N. (2025). *Utilizing Generative AI for Cyber Defense Strategies*, IGI Global, Hershey, USA.
13. Aml Expert. (2017). Anti money laundering exam : study guide & practice exam. Createspace Independent Publishing Platform.
14. CipherTrace (2021). Cryptocurrency Crime and Anti-Money Laundering Report, Cryptocurrency Intelligence February 2021.
15. Chau, D. (2018). *Anti-money laundering transaction monitoring systems implementation finding anomalies*. John Wiley & Sons, Inc.
16. Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering. *IEEE Access*, 9, 18481–18496. https://doi.org/10.1109/access.2021.3052313

THE ROLE OF ARTIFICIAL INTELLIGENCE TOOLS IN THE FIGHT AGAINST MONEY LAUNDERING AND THE FINANCING OF TERRORISM IN THE MODERN DIGITAL ENVIRONMENT

Aleksandar Petković

Radovan Vladisavljević

Petar Ciganović

Abstract: *The fight against money laundering and terrorist financing gains a new dimension with the advent of digital currencies. Digital currencies also include cryptocurrencies, which very quickly attract a large number of users, mostly legitimate users. Due to their nature, cryptocurrencies are becoming a preferred vehicle for money laundering and terrorist*

financing (AML/CFT). Cryptocurrencies themselves rely heavily on pseudo-anonymity as well as high transaction speed. Namely, the volume and speed of transactions greatly complicates the work of agencies tasked with fighting money laundering and terrorist financing. The emergence of artificial intelligence as well as specialized tools based on artificial intelligence greatly help agencies to more quickly and accurately locate transactions that can be linked to money laundering and terrorist financing.

***Keywords**: artificial intelligence, fight against money laundering and money financing, cryptocurrencies, blockchain.*