Izv. prof. dr. sc. Marko Perkušić*
Izv. prof. dr. sc. Šime Jozipović**
Luka Roso, mag. iur.***

PRAVNI POLOŽAJ VIRTUALNIH VALUTA U MEĐUNARODNIM HAKERSKIM NAPADIMA KOJIMA SE FINANCIRAJU TERORISTIČKE AKTIVNOSTI I ODMETNUTE DRŽAVE[1]

UDK / UDC: *336.74 : 004.056.5*
336.74 : 343.9.024
341.4 : 343.9.024
DOI: *10.31141/zrpfs/2263*
Izvorni znanstveni rad / Original scientific paper
Primljeno / Received: 11.9.2025.
Prihvaćeno / Accepted: 1.9.2026.

Rad analizira globalne izazove u regulaciji kriptoimovine, s posebnim naglaskom na suzbijanje cyber-kriminala i nezakonitih financijskih aktivnosti. Od pojave Bitcoina 2008. godine, tržište kriptoimovine bilježi dinamičan rast te privlači sve veći interes fizičkih osoba, poslovnih subjekata i institucionalnih ulagača. Većina je gospodarske aktivnosti vezane za kriptoimovinu zakonita. Međutim, decentralizirana i pseudonimna priroda kriptoimovine čini je pogodnom za zlouporabe i ilegalne aktivnosti poput pranja novca, prijevara, iznuda i financiranja terorizma. Unatoč određenom napretku u regulaciji, učinkovito nadziranje i provedba propisa teško su ostvarivi bez snažne međunarodne suradnje.

U radu se polazi od teze da postojeći regulatorni mehanizmi nisu dostatni zbog globalnog karaktera kriptotransakcija. Rad analizira načine na koje kriminalne skupine dolaze do kriptoimovine poput hakerskih napada, socijalnog inženjeringa i drugih oblika računalnog kriminala. U tom kontekstu ukazuje se na izazove s kojima se međunarodna zajednica suočava u praćenju ilegalnih aktivnosti, osobito u vezi s državama u kojima nedostaje sustavna institucionalna kontrola ili koje predstavljaju tzv. odmetnute države (rogue states). Bazirano na ovoj strukturi, provodi se analiza postojećeg međunarodnog pravnog okvira, s naglaskom na mjere za sprečavanje pranja novca (AML) i financiranja terorizma. Zaključno, rad ističe potrebu za koherentnijim, bolje usklađenim i učinkovitijim međunarodnim regulatornim pristupima.

* Izv. prof. dr. sc. Marko Perkušić, izvanredni profesor na Katedri za pravne znanosti pri Fakultetu za forenzičke znanosti Sveučilišta u Splitu. Ruđera Boškovića 33, 21000 Split, Republika Hrvatska. E-mail: mperkusi@forenzika.unist.hr. ORCID: 0000-0002-5845-2961.

** Izv. prof. dr. sc. Šime Jozipović, Sveučilište u Splitu, Ekonomski fakultet, Cvite Fiskovića 5, Split, Republika Hrvatska, e-mail: sime.jozipovic@efst.hr, ORCID: 0000-0002-8050-5134.

*** Luka Roso, mag. iur., asistent na Katedri za međunarodno javno pravo Pravnog fakulteta Sveučilišta u Splitu. Domovinskog rata 8, 21000 Split, Republika Hrvatska. E-mail: luka.roso@pravst.hr. ORCID: 0009-0008-5892-0877.

[1] Ovaj rad nastao je u sklopu projekta Sveučilišta u Splitu Društvene dimenzije monetarne i digitalne transformacije (DDMDT, IP-UNIST-02).

Ključne riječi: *AML, sprečavanje pranja novca, kriptovalute, kriptoimovina, kibernetički kriminal*

1. UVOD

Od predstavljanja koncepta Bitcoina kao prve kriptovalute 2008. godine do danas,[2] tržište kriptoimovine doživjelo je značajne promjene. S vremenom su razvijeni programabilni oblici kriptoimovine,[3] implementirani prvi pametni ugovori[4] te su se otvorile mogućnosti za primjenu decentraliziranih aplikacija, decentraliziranog odlučivanja i financijskih usluga.[5] Rastući interes za kriptoimovinu potaknuo je ulazak sve više malih ulagača, ali i institucionalnih investitora u ovo tržište. Paralelno s tim procesom postupno se provodila i regulacija tržišta, osobito u razvijenim ekonomijama poput Europske unije.

Posebice u ranim fazama, kriptovalute poput Bitcoina često su korištene za ilegalne aktivnosti, uključujući kupnju zabranjenih dobara i usluga, kao i za pranje novca stečenog računalnim kriminalom.[6] S vremenom je legalno tržište kriptovaluta dobilo sve veći značaj, a mnoge države stvorile su niz alata za zaštitu od zlouporabe tih tehnologija.[7] Ipak, zbog inherentne decentraliziranosti,[8] kriptoimovina ostaje

---

[2] Vidjeti: Doguet, J. J., *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 2013., Louisiana Law Review, vol. 73.; Pflaum, I.; Hateley, E., *A bit of a problem: National and extraterritorial regulation of virtual currency in the age of financial disintermediation*, 2014., Georgetown Journal of International Law, vol. 45; Perkušić, M., *Pravo elektroničkog plaćanja*, 2020., Školska knjiga, Zagreb, str. 310-326.

[3] Vidjeti *infra* poglavlje 2.

[4] Pametni ugovor može se definirati kao „računalni program koji se upotrebljava za automatizirano izvršenje sporazuma ili njegova dijela, pri čemu se upotrebljava slijed elektroničkih zapisa podataka i osigurava njihova cjelovitost i točnost kronološkog redoslijeda". Čl. 2. st. 39. Uredbe (EU) 2023/2854 Europskog parlamenta i Vijeća od 13. prosinca 2023. o usklađenim pravilima za pravedan pristup podacima i njihovu uporabu i o izmjeni Uredbe (EU) 2017/2394 i Direktive (EU) 2020/1828 (2023/2854, 22. 12. 2023.). Opširnije o pametnim ugovorima vidjeti Perkušić, M., *The Legal Treatment of Smart Contracts under Croatian Law* // Zbornik radova Pravnog fakulteta u Splitu, 61 (2024.), 4; 473-497. doi: 10.31141/zrpfs.2024.61.154.473.

[5] Opširnije o decentraliziranosti virtualnih valuta vidjeti Jozipović, Š.; Perkušić, T.; Keršić, M. (2025.), *Digitalni euro i kriptovalute: Sličnosti i moguće analogije za pravnu regulaciju*, u: Perkušić, M.; Jozipović, Š.; Pečarić, M. (ur.), „*Digitalni euro i bezgotovinsko plaćanje: pravna regulacija i utjecaj na financijski sustav*", Sveučilište u Splitu, str. 179-182.

[6] Vidjeti primjerice: Raeesi, R., *The silk road, bitcoins and the global prohibition regime on the international trade in illicit drugs: can this storm be weathered?*, 2015., Glendon Journal of International Studies 8.1-2; Martin, J., *Lost on the Silk Road: Online drug distribution and the 'cryptomarket'*, 2014., Criminology & Criminal Justice 14, no. 3, str. 351-367.

[7] Vidjeti primjerice: Emmert, F., *The regulation of cryptocurrencies in the United States of America*, European Journal of Law Reform 25 (2023.): 1-2. ; Riley, J., *The current status of cryptocurrency regulation in China and its effect around the world,* China and WTO Review 7.1 (2021): 135-152.

[8] Kod decentraliziranih kriptovaluta/kriptoimovine ne postoji središnje tijelo, kao ni odgovorna osoba. Opširnije o tome vidjeti: Dourado, E.; Brito, J., 2014. *Cryptocurrency*. U: *The New Palgrave Dictionary of Economics*; Gikay, A. A., *Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union Law*, 2018., Journal of Law, Technology & the Internet, Vol. 9; Perkušić, M., *Pravo elektroničkog plaćanja*, 2020., Školska knjiga, Zagreb, str. 311-313.

globalni fenomen koji je nemoguće regulirati i nadzirati isključivo lokalno.[9] Uspješna borba protiv nezakonitih aktivnosti povezanih s kriptoimovinom zahtijeva dobro koordiniranu međunarodnu suradnju.

Mnoge države sudjeluju u međunarodnim inicijativama, poput Financial Action Task Force (FATF), kako bi otkrile nezakonite aktivnosti i pratile povezane financijske tokove.[10] No, upravo potreba za suradnjom predstavlja jedan od ključnih izazova jer se terorističke skupine često nalaze na teritorijima s nedostatnom kontrolom države, dok pojedine države koje su isključene iz međunarodne zajednice (tzv. *rogue states*)[11] aktivno podupiru računalni kriminal kao izvor vlastitih prihoda. Naime, takve države često ili izravno organiziraju operacije računalnog kriminala u drugim državama, ili sudjeluju u realiziranim prihodima od računalnog kriminala, a zauzvrat kriminalcima nude utočište te mogućnost da ilegalno stečena sredstva troše bez straha od progona. Ovaj se rad fokusira upravo na problem manjka međunarodne suradnje i ulogu odmetnutih država u borbi protiv određenih oblika računalnog kriminala povezanog s kriptoimovinom.

U uvodnom dijelu rada bit će predstavljen pravni položaj kriptoimovine, s posebnim osvrtom na njezin status unutar Europske unije i međunarodne zajednice. Zatim će se predstaviti kako zločinačke organizacije putem raznih kaznenih djela poput krađe, prijevare ili iznude dolaze do značajnih sredstava u obliku kriptoimovine. U ovome dijelu rada prezentirat će se mehanizmi stjecanja protupravne materijalne koristi, odnosno hakerski napadi, socijalni inženjering i druge povezane metode.

Na temelju prikazanih slučajeva, u radu se zatim analizira međunarodni pravni okvir za borbu protiv takvih aktivnosti, s naglaskom na mjere za sprečavanje financiranja terorizma i pranja novca. Posebno će se obraditi problem zaobilaženja međunarodnih financijskih kanala putem kriptotransakcija i izazovi s kojima se međunarodna zajednica suočava u svojim nastojanjima da spriječi prijenos ilegalno stečenih sredstava na virtualne novčanike ili račune zločinačkih organizacija i terorističkih skupina. Zaključno, rad daje pregled ključnih slabosti postojećeg međunarodnog pravnog okvira u odnosu na kriptoimovinu.

[9] Vidjeti Vuletić, D., *Pravna priroda kriptoimovine u pravu Europske unije i hrvatskom pravu*, Zbornik radova Pravnog fakulteta u Tuzli 10.1 (2024): 67-94.

[10] Opširnije o Financial Action Task Force (FATF) vidjeti *infra* poglavlje 4.1.

[11] Pojam „odmetnute države" (engl. *rogue states*) označava države koje se percipiraju kao sustavni prekršitelji temeljnih normi međunarodnog poretka i kao prijetnja međunarodnoj sigurnosti, osobito zbog potpore terorizmu, razvoja ili širenja oružja za masovno uništenje te agresivnog djelovanja prema drugim državama. Pojam prije svega predstavlja međunarodnu – političku kategoriju, dok pravne posljedice manjka suradnje s drugim državama proizlaze iz odredbi pojedinih međunarodnih konvencija ili drugih pravnih akata. Vezano za rogue state, vidjeti primjerice: O'Reilly, K. P. (2007.). *Perceiving Rogue States: The Use of the 'Rogue State' Concept by U.S. Foreign Policy Elites*, Foreign Policy Analysis.

2. KRIPTOIMOVINA

Kriptoimovina je na području Europske unije regulirana Uredbom o tržištima kriptoimovine (Markets in Crypto-Assets Regulation – MiCAR).[12] Pritom navedena Uredba definira kriptoimovinu kao „digitalni prikaz vrijednosti ili prava koje se može prenositi i pohranjivati elektronički, s pomoću tehnologije distribuiranog zapisa ili slične tehnologije".[13] Uz to, Uredba regulira i nekoliko vrsta kriptoimovine kao što su: token vezan uz imovinu,[14] token elektroničkog novca[15] i korisnički token,[16] ali smatramo da se pritom, shodno Uredbi, osnovna podjela vrsta kriptoimovine može izvršiti na tokene vezane uz imovinu i elektronički novac, te na one tokene koji nisu uz njih vezani.[17] Činjenice da Uredba MiCAR ne uređuje sve aspekte kriptoimovine bili su svjesni i njezini regulatori pa se tako u Uredbi ističe kako se ne primjenjuje na kriptoimovinu koja je jedinstvena i ne može se zamijeniti drugom kriptoimovinom[18] [19] te na kriptoimovinu koja se kvalificira kao financijski instrumenti, depoziti, uključujući strukturirane depozite, novčana sredstva (osim ako se kvalificiraju kao tokeni e-novca) itd.[20]

Iz navedenoga proizlazi kako se Uredba fokusira na tri vrste tokena koji se smatraju kriptoimovinom. Prva kategorija bili bi tokeni čija se vrijednost nastoji održati stabilnom vezivanjem za određenu službenu valutu (token e-novca). Primjer takve kriptoimovine bio bi EUROe, vrsta tzv. stablecoina čija je vrijednost vezana 1:1 uz euro i koji je u cijelosti podržan fiat sredstvima na računu u eurozoni.[21] Druga kategorija tokena odnosila bi se na tokene vezane uz imovinu (vežu se uz drugu vrijednost ili pravo odnosno njihovu kombinaciju, uključujući jednu ili više službenih valuta), a primjer takvog tokena bili bi stablecoini čija se vrijednost veže

---

[12] Uredba (EU) 2023/1114 Europskog parlamenta i Vijeća od 31. svibnja 2023. o tržištima kriptoimovine te izmjeni uredbi (EU) br. 1093/2010 i (EU) br. 1095/2010 i direktiva 2013/36/EU i (EU) 2019/1937 (MiCAR).

[13] Čl. 3. st. 1. t. 5. MiCAR. Osim navedene definicije, postoje i razne druge definicije kriptoimovine koje prije svega proizlaze iz pravne znanosti pa se tako kriptoimovina definira i kao „skup elektronički prenosivih i kriptički zaštićenih subjektivnih imovinskih prava u digitalnom prikazu koja imaju jednog nositelja". Vuletić, D., *Pravna priroda kriptoimovine u pravu Europske unije i hrvatskom pravu*, Zbornik radova Pravnog fakulteta u Tuzli 10.1 (2024.), str. 81.

[14] Čl. 3. st. 1. t. 6. MiCAR, definira tokene vezane uz imovinu kao vrstu kriptoimovine koja nije token elektroničkog novca i čija se vrijednost nastoji održati stabilnom vezivanjem uz drugu vrijednost ili pravo odnosno njihovu kombinaciju, uključujući jednu ili više službenih valuta.

[15] Čl. 3. st. 1. t. 7. MiCAR, definira tokene elektroničkog novca (token e-novca) kao vrstu kriptoimovine čija se vrijednost nastoji održati stabilnom vezivanjem uz vrijednost jedne službene valute.

[16] Čl. 3. st. 1. t. 9. MiCAR, definira korisnički token kao vrstu kriptoimovine koja služi samo za davanje pristupa robi ili usluzi koju pruža njegov izdavatelj.

[17] Navedeno proizlazi i iz čl. 1. st. 1. MiCAR.

[18] Stoga Uredbom nisu regulirani tzv. nezamjenjivi tokeni (*non-fungible tokens – NFT*) koji su jedinstveni i predstavljaju zaseban digitalni objekt. Opširnije o NFT-ovima vidjeti: Wang, Q.; Li. R. Wang; Q. & Chen, S. (2021.). *Non-fungible token (NFT): Overview, evaluation, opportunities and challenges*. arXiv preprint arXiv:2105.07447; Taherdoost, H. (2022.), *Non-fungible tokens (NFT): A systematic review*. Information, 14(1), 26.

[19] Čl. 2. st. 3. MiCAR.

[20] Čl. 2. st. 4. MiCAR.

[21] Vidjeti: EUROe, dostupno na: https://www.euroe.com/ (pristupljeno 25. srpnja 2025.).

uz više vrsta imovine, npr. kombinaciju fiat valuta (50 % EUR + 50 % USD), roba (zlato/srebro) ili drugih kriptoimovina. Kao slučajeve iz prakse za takvu vrstu tokena možemo navesti: Diem (bivši Libra – projekt Meta/Facebooka),[22] Tether Gold (XAUT),[23] DAI (MakerDAO)[24] i sUSD (Synthetix).[25] Treća kategorija tokena odnosila bi se na ostale tokene kriptoimovine koji nisu vezani uz prethodno navedenu vrstu imovine te nisu ni isključeni samom Uredbom. U tu kategoriju spadaju brojne kriptovalute poput Bitcoina[26] i Ethera[27] [28] jer služe kao sredstvo razmjene, ulaganja ili pohrane vrijednosti. Dakle, kod treće kategorije riječ je o kriptoimovini koja nema nikakvo pokriće, te joj se cijena formira slobodno na tržištu, a koristi se u različite svrhe, od sredstva razmjene do pristupa uslugama.

Kako se Uredba fokusirala na tri navedene vrste tokena, tako je svaki od njih i posebno regulirala. Pri tom se, shodno odredbama Uredbe, kao ključne karakteristike tokena e-novca ističu: - izdavatelji tokena e-novca (može ih izdavati kreditna institucija ili ovlaštena institucija za e-novac),[29] -obvezna autorizacija i nadzor koje provode nacionalna nadležna tijela uz određenu ulogu Europskog nadzornog tijela za bankarstvo (EBA) kada je token sistemski značajan,[30] - obvezno pravo na izdavanje i iskup po nominalnoj vrijednosti,[31] - obveza izdavanja bijele knjige (stroži

---

[22] Opširnije o tome vidjeti: Pupolizio, I. (2022.), *From libra to diem. the pursuit of a global private currency*. Global Jurist, 22(2), 281-306.

[23] U ovom slučaju svaki token predstavlja jednu uncu zlata koja je pohranjena u trezoru te u biti kad imate jedan takav token, vlasnik ste jedne unce zlata. Vidjeti opširnije *Tether Gold* (XAUT), dostupno na: https://gold.tether.to/ (pristupljeno 25. srpnja 2025.).

[24] Iako je vrijednost DAI-a vezana uz američki dolar, riječ je o decentraliziranom stablecoinu koji ne podupire fiat novac, već kolateral u kriptoimovini. Opširnije vidjeti: DAI (MakerDAO) dostupno na: https://makerdao.com/en/ (pristupljeno 25. srpnja 2025.).

[25] Slično kao i kod DAI-a, riječ je o sintetičkom stablecoinu koji funkcionira unutar Synthetix protokola, te je vezan uz američki dolar i kolateral je osiguran kriptoimovinom. Opširnije vidjeti: *sUSD (Synthetix)*, dostupno na: https://www.synthetix.io/ (pristupljeno 25. srpnja 2025.).

[26] Bitcoin se može definirati kao decentralizirana virtualna valuta (kriptovaluta), koja omogućuje peer-to-peer prijenos vrijednosti bez potrebe za posrednicima. Navedeno se odvija putem blockchain tehnologije pomoću koje se podaci snimaju na distribuiranom serveru. Opširnije vidjeti: Nakamoto, S. (2008.), *Bitcoin: A peer-to-peer electronic cash system*; Perkušić, M., *Pravo elektroničkog plaćanja*, 2020., Školska knjiga, Zagreb, str. 311.

[27] Ethereum se može definirati kao decentralizirana blockchain platforma s integriranim pametnim ugovorima. Kriptovaluta (kriptotoken) koja se koristi na navedenoj platformi jest Ether (ETH) koji je prvenstveno namijenjen plaćanju transakcijskih naknada (gas) i obavljanju aktivnosti na mreži. S obzirom na programibilnost sustava putem platforme Ethereum, moguće je stvoriti niz drugih tokena koji se koriste u raznovrsne svrhe, npr. kao sredstvo plaćanja ili dokaz o vlasništvu. Opširnije o Ethereumu vidjeti: Tikhomirov, S. (2017, October), *Ethereum: state of knowledge and research perspectives*, in International symposium on foundations and practice of security (pp. 206-221). Cham: Springer International Publishing; Arslanian, H. (2022.), *Ethereum. In The book of crypto: The complete guide to understanding bitcoin, cryptocurrencies and digital assets* (pp. 91-98). Cham: Springer International Publishing.

[28] Vidjeti Vuletić, D., *Pravna priroda kriptoimovine u pravu Europske unije i hrvatskom pravu,* Zbornik radova Pravnog fakulteta u Tuzli 10.1 (2024.), str. 86.

[29] Čl. 48. st. 1. t. a) MiCAR.

[30] Tako su za nadzor u Republici Hrvatskoj zaduženi Hrvatska agencija za nadzor financijskih usluga i Hrvatska narodna banka. Vidjeti čl. 6. st. 1. Zakona o provedbi Uredbe (EU) 2023/1114 o tržištima kriptoimovine (NN 85/24).

[31] Čl. 49. MiCAR.

zahtjevi nego za druge dvije kategorije tokena),[32] te - zabrana kamate[33]. Karakteristike tokena vezanih uz imovinu slične su onima tokena e-novca uz činjenicu da su kriteriji za tokene vezane uz imovinu, shodno Uredbi, blaži nego za tokene e-novca. Tako tokene vezane uz imovinu može izdavati širi krug osoba nego tokene e-novca, uz uvjet da su tražili odobrenje od nadležnog tijela.[34] Također, moraju imati bijelu knjigu i plan upravljanja rezervama, ali su kriteriji blaži nego za tokene e-novca.[35] Izdavatelji tokena vezanih uz imovinu moraju održavati kapitalne zahtjeve propisane Uredbom,[36] te moraju uspostaviti djelotvoran sustav upravljanja koji mora biti u stanju ispuniti organizacijske zahtjeve propisane Uredbom.[37] Uz to moraju osigurati da imovina koja osigurava tokene bude likvidna, sigurna i odvojena od vlastite imovine izdavatelja.[38] U slučaju da je token vezan uz imovinu sistemski značajan, bit će potreban stroži nadzor Europskog nadzornog tijela za bankarstvo (EBA).[39] Za ostale tokene kriptoimovine potrebno je zadovoljiti najniže kriterije, jer Uredba MiCAR prema njima ima najblaži režim. Tako je izdavatelj ostalih tokena kriptoimovine prije ponude tokena javnosti ili prijema za trgovanje dužan[40] objaviti bijelu knjigu,[41] te izdavatelj mora obavijestiti nadležno tijelo o objavi bijele knjige, ali ne mora tražiti odobrenje da bi to učinio[42]. Uredba još propisuje nadzor nad marketingom (promidžbenim sadržajem) za ostale tokene kriptoimovine,[43] ali se pri tom na izdavatelje ne primjenjuju strogi kapitalni i likvidnosni zahtjevi kao na izdavatelje prethodno navedenih tokena. Stoga možemo zaključiti kako se za ostale tokene kriptoimovine ostavlja najviše prostora za određene inovacije, ali se Uredbom ipak želio uvesti određeni stupanj transparentnosti i spriječiti (koliko je to moguće) manipulacije na tržištu.

2.1. Kriptoimovina kao objekt ilegalnih aktivnosti

U pravnom se sustavu Republike Hrvatske kriptoimovina sve češće pojavljuje kao središnji element u kaznenim predmetima, i to kao objekt nad kojim je izvršeno kazneno djelo ili kao sredstvo izvršenja kaznenog djela.

---

[32] Osim elemenata propisanih za sve kriptoimovine, bijela knjiga za tokene e-novca mora sadržavati i dodatne kriterije propisane čl. 51. Uredbe MiCAR.

[33] Čl. 50. MiCAR.

[34] Čl. 16. MiCAR.

[35] Vidjeti čl. 19. MiCAR.

[36] Shodno čl. 35. MiCAR, izdavatelji tokena vezanih uz imovinu moraju održavati stalni minimalni iznos vlastitih sredstava, i to u većem iznosu od 350.000 eura ili 2 % prosječne vrijednosti imovine rezervi (*reserve assets*).

[37] Vidjeti čl. 34. MiCAR.

[38] Čl. 36.-38. MiCAR.

[39] Vidjeti čl. 43. – 45. MiCAR.

[40] Postoji i iznimka od obveze objave bijele knjige, pa tako shodno čl. 4. st. 2. t. b MiCAR, ne treba objaviti bijelu knjigu ako vrijednost tokena koji se nudi ne prelazi iznos od 1 milijun eura u razdoblju od 12 mjeseci.

[41] Sadržaj i oblik bijele knjige o kriptoimovini za ostale tokene kriptoimovine propisan je čl. 6. Uredbe MiCAR.

[42] Čl. 8. st. 3. MiCAR.

[43] Vidjeti čl. 7. MiCAR.

Unatoč svojoj digitalnoj i decentraliziranoj prirodi, kriptoimovina predstavlja dio imovine njezina imatelja.[44] Stoga ona u načelu podliježe i imovinskopravnoj zaštiti. Kao objekt kaznenog djela, stjecanje tuđe kriptoimovine može biti neposredni cilj protupravnog djelovanja. To bi, primjerice, bio slučaj kada osoba neovlašteno prisvoji tuđu kriptovalutu upotrebom zlonamjernog softvera, socijalnog inženjeringa[45] ili iskorištavanjem sigurnosnih propusta platformi za trgovanje ili pohranu. Takva ponašanja u kaznenom pravu mogu biti kvalificirana kao jedno ili više sljedećih kaznenih djela: krađa (čl. 228 Kaznenog zakona),[46] računalna prijevara (čl. 271 KZ-a), neovlašteni pristup računalnom sustavu (čl. 266 KZ-a) ili uništenje i oštećenje podataka (čl. 268 KZ-a), ovisno o konkretnom načinu izvršenja.

Kao sredstvo kaznenog djela, kriptoimovina sve se više koristi u svrhu prikrivanja tragova počinjenih kaznenih djela, financiranja nezakonitih aktivnosti ili u procesu pranja novca. Sudjelovanje u sustavu kriptoimovine, iako tehnički složeno, moguće je bez posrednika, u potpunosti decentralizirano. Nadalje, zbog pseudonimnosti digitalnih novčanika i spomenute tehničke mogućnosti za obavljanje transakcija bez posrednika, kriptovalute omogućuju stvaranje složenih struktura transfera sredstava koje je teško pratiti. Štoviše, kako bi se dodatno otežalo praćenje, često se koriste posebne usluge posrednika za zamaskiranje transakcija ili kriptografski mehanizmi pojedinih kriptovaluta za prikrivanje iznosa transakcije. U kontekstu kaznenog prava, ovi mehanizmi koriste se za ostvarenje oblika pranja novca (čl. 265 Kaznenog zakona).

3. HAKERSKI NAPADI I SOCIJALNI INŽENJERING U SFERI KRIPTOIMOVINE

Jedna od temeljnih zadaća države jest zaštita imovinskih prava svojih građana.[47] Ona se ostvaruje uspostavom učinkovitih građanskopravnih, kaznenopravnih i postupovnih mehanizama kojima se sprečava neovlašteno oduzimanje imovine te

[44] Vidjeti mišljenje porezne uprave kl. 410-01/17-08/29, br. 513-07-21-01/18-4, „Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama".

[45] Socijalni inženjering (engl. *social engineering*) predstavlja skup tehnika kojima napadač, putem psihološke manipulacije, navodi ljude na otkrivanje povjerljivih podataka, omogućavanje neovlaštenog pristupa sustavu ili poduzimanje druge radnje koja ugrožava informacijsku sigurnost. Za razliku od napada koji se primarno temelje na iskorištavanju tehničkih nedostataka, socijalni inženjering usmjeren je na ljudski čimbenik kao potencijalno najslabiju kariku sigurnosnog sustava. O socijalnom inženjeringu detaljnije: Wang, Z.; Sun, L. i Zhu, H. (2020.), „Defining Social Engineering in Cybersecurity," *IEEE Access*, 8, 85094–85115.

[46] Kazneni zakon – KZ, NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24.

[47] Vidjeti primjerice čl. 48 i slj. Ustav RH, NN 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14; Protokol br. 1 uz Konvenciju za zaštitu ljudskih prava i temeljnih sloboda, Pariz, 20. ožujka 1952., ETS br. 009, stupio na snagu 18. svibnja 1954.

omogućuje povrat imovine i naknada štete.[48] Samo u državama u kojima postoji jasno definirana institucionalna zaštita vlasništva i drugih imovinskih prava mogu se nesmetano razvijati gospodarske aktivnosti. Sve izraženija uloga digitalne ekonomije potaknula je cijeli niz zakonodavnih i administrativnih inicijativa koje služe upravo uspostavi pouzdanog i sigurnog okruženja za gospodarske aktivnosti na internetu. Tako je Europska unija donijela brojne pravne akte koji su u cijelosti ili dijelom usmjereni na stvaranje veće pravne sigurnosti transakcija u digitalnom okruženju.[49] Pravna sigurnost u tom smislu podrazumijeva mogućnost identifikacije odgovornih subjekata, utvrđivanja primjenjivog prava i nadležnog tijela te postojanje učinkovitih pravnih sredstava u slučaju neovlaštenog raspolaganja digitalnom imovinom.

Međutim, dok se nad centraliziranim sustavima plaćanja može provoditi učinkovita regulacija, decentralizirana priroda kriptoimovine znatno otežava nadzor svih aktera uključenih u stvaranje, pohranu i transakcije kriptoimovinom. Europska unija je, kako smo ranije istaknuli, ovu problematiku nastojala urediti donošenjem Uredbe MiCAR, koja opsežno regulira postupanje relevantnih aktera na njezinu području. Predmetna Uredba, međutim, obvezuje samo subjekte koji djeluju unutar pravnog okvira Europske unije, a njezin je stvarni doseg ograničen činjenicom da se mnoge nezakonite aktivnosti odvijaju putem globalno decentraliziranih mreža ili su vezane uz tehnološku infrastrukturu u državama koje ne osiguravaju usporedivu razinu regulatorne zaštite. Stoga se hakerski napadi i drugi oblici računalnog kriminala u pravilu koordiniraju i izvode s područja država u kojima ne postoje funkcionalni pravni sustavi utemeljeni na vladavini prava. Takva situacija otvara problem prekogranične nadležnosti jer se počinitelj, žrtva, računalni sustav i imovina

[48] Uz negativnu obvezu suzdržavanja od neopravdanih zahvata u pravo vlasništva, iz čl. 1. Protokola br. 1 uz Konvenciju za zaštitu ljudskih prava i temeljnih sloboda za državu proizlaze i pozitivne obveze zaštite imovine od protupravnih zahvata trećih osoba, uključujući obvezu osiguranja djelotvornih pravnih sredstava kojima oštećenik može ishoditi utvrđenje povrede i zaštitu svojih prava. Vidjeti primjerice presudu Europskog suda za ljudska prava u predmetu *Blumberga protiv Latvije*, zahtjev br. 70930/01, od 14. listopada 2008., t. 67.

[49] Vidjeti primjerice: Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (27.12.2022, L 333/1) – DORA; Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištima financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (MiFID II); Uredba (EU) 2019/2088 Europskog parlamenta i Vijeća od 27. studenoga 2019. o objavljivanju informacija povezanih s održivošću u sektoru financijskih usluga (SFDR); Uredba (EU) 2023/988 Europskog parlamenta i Vijeća od 10. svibnja 2023. o općoj sigurnosti proizvoda, izmjeni Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća i Direktive (EU) 2020/1828 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2001/95/EZ Europskog parlamenta i Vijeća i Direktive Vijeća 87/357/EEZ; Uredba (EU) 2014/910 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (eIDAS), izmijenjena Uredbom (EU) 2024/1183 ; Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama); Direktiva (EU) 2019/2161 Europskog parlamenta i Vijeća od 27. studenoga 2019. o izmjeni Direktive Vijeća 93/13/EEZ i direktiva 98/6/EZ, 2005/29/EZ te 2011/83/EU Europskog parlamenta i Vijeća u pogledu boljeg izvršavanja i modernizacije pravila Unije o zaštiti potrošača (Direktiva o modernizaciji); Direktiva (EU) 2023/2673 Europskog parlamenta i Vijeća od 22. studenoga 2023. o izmjeni Direktive 2011/83/EU u pogledu ugovora o financijskim uslugama sklopljenih na daljinu te o stavljanju izvan snage Direktive 2002/65/EZ; Direktiva 2015/2366/EU Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu (PSD2).

koja je predmet napada mogu nalaziti u različitim državama. Posljedično, kazneni je progon u takvim slučajevima često ovisan o međunarodnoj pravnoj pomoći, razmjeni elektroničkih dokaza, identifikaciji stvarnih počinitelja i spremnosti strane države na suradnju.[50]

Žrtve se, s druge strane, često nalaze upravo u razvijenim državama. Nakon uspješno provedenog napada kriminalne organizacije koriste decentralizirana sredstva plaćanja radi prikrivanja tragova te prijenosa sredstava na račune u državama koje ne surađuju s pravosudnim tijelima država u kojima je kazneno djelo počinjeno.

Modus operandi zločinačkih organizacija naročito je vidljiv u kontekstu računalnog kriminala blisko vezanog uz kriptoimovinu. Naime, s obzirom na to da je kriptoimovina po svojoj prirodi izrazito internacionalizirana, čak i kvalitetna nacionalna odnosno supranacionalna zaštita ne može u potpunosti spriječiti nastanak štete uslijed hakerskih napada, socijalnog inženjeringa ili softvera za iznudu (engl. *ransomware*). U nastavku će se stoga prikazati dva ogledna slučaja iz ove sfere, koji će u kasnijim dijelovima rada poslužiti kao podloga za analizu postojećih pravnih mehanizama zaštite te dosega međunarodnih inicijativa za borbu protiv računalnog kriminala.

3.1. Slučaj grupe Lazarus i napad na mrežu Ronin

Proteklih godina proveden je cijeli niz hakerskih napada na različite sustave u sektoru kriptoimovine. Kao primjer iznimno štetnog hakerskog napada u kojemu je korištena kombinacija socijalnog inženjeringa i sofisticiranih hakerskih alata, ističe se napad na tzv. Mrežu Ronin u ožujku 2022. godine. Navedena mreža, kojom upravlja trgovačko društvo Sky Mavis, predstavlja tehnološki temelj za decentraliziranu aplikaciju (tzv. dApp)[51] Axie Infinity, koja je u to vrijeme bila vodeća decentralizirana računalna igra.[52] Mreža Ronin funkcionirala je kao tehnološka infrastruktura putem koje su se evidentirali i odobravali prijenosi digitalne imovine povezani s aplikacijom. Stoga je kontrola nad mrežom omogućavala odobravanje i blokiranje transakcija. Drugim riječima, subjekti koji su kontrolirali mrežu mogli su odobravati kako legitimne, tako i neosnovane transakcije te time faktički raspolagati sredstvima drugih sudionika unutar mreže. Ovo, međutim, nije predstavljalo problem

[50] Temeljni multilateralni instrument u ovom području jest Konvencija Vijeća Europe o kibernetičkom kriminalu (tzv. Budimpeštanska konvencija), Budimpešta, 23. studenoga 2001., ETS br. 185, koja uz materijalnopravne i postupovne odredbe sadržava i mehanizme međunarodne suradnje, uključujući uzajamnu pravnu pomoć te hitno očuvanje pohranjenih računalnih podataka. Republika Hrvatska potvrdila ju je Zakonom o potvrđivanju Konvencije o kibernetičkom kriminalu, NN – Međunarodni ugovori, br. 9/02.

[51] O funkcijama i ulozi dApp-a vidjeti primjerice: Leiponen, A.; Llewellyn, D. W. T.; Wang, Q., *The dApp economy: A new platform for distributed innovation?*. Innovation 24, no. 1 (2022): 125-143.

[52] Alam, O., *Understanding the economies of blockchain games: An empirical analysis of Axie Infinity*. Distributed Computing Group Computer Engineering and Networks Laboratory ETH Zürich, 2022., URL: https://pub.tik.ee.ethz.ch/students/2 (2022.), str. 5 i slj.

za vrijeme uobičajenog korištenja mreže jer su svi subjekti bili verificirane osobe sa značajnim interesom u tome da sustav pouzdano funkcionira.

U sklopu napada otuđeno je ukupno 173.600 jedinica kriptovalute Ether (ETH) i 25,5 milijuna USDC tokena, u ukupnoj protuvrijednosti od gotovo 625 milijuna američkih dolara u trenutku incidenta. Napad je označen kao jedan od najznačajnijih hakerskih upada u povijesti decentraliziranih financija (DeFi), a istraživala su ga različita pravosudna i regulatorna tijela. Tako su u SAD-u Agencija za kibernetičku sigurnost i sigurnost infrastrukture (CISA), Federalni istražni ured (FBI) i Ministarstvo financija SAD-a objavili zajednički savjetodavni dokument AA22-108A kojim se opisuju aktivnosti vezane uz navedeni napad.[53] Ovaj savjetodavni dokument nema karakter obvezujućeg pravnog izvora, već služi informiranju javnih i privatnih subjekata o utvrđenom obrascu prijetnje, metodama napada i preporučenim mjerama zaštite.

U zajedničkom savjetodavnom dokumentu navedena tijela iznose kako su kibernetički napad predvodili sjevernokorejski državni akteri povezani s tzv. Grupom Lazarus. Pri tome zaključuju kako je ovaj napad predstavljao dio šireg obrasca usmjeravanja hakerskih napada na infrastrukturu povezanu s kriptoimovinom. Početna izvješća ukazivala su na obrazac sofisticiranih napada temeljenih na socijalnom inženjeringu. Cilj napada bio je navesti osobe koje su držale kriptoimovinu ili bile povezane s kriptoprojektima da preuzmu naizgled legitimne aplikacije za trgovanje kriptovalutama u koje je bio ugrađen zlonamjerni softver.[54] Naime, za provedbu navedenih napada korišten je skup zlonamjernih softverskih aplikacija pod nazivom „TraderTraitor". Štetni računalni kod distribuiran je putem naizgled vjerodostojnih internetskih stranica, osmišljenih tako da obmanu korisnike i potaknu ih na njegovo dobrovoljno preuzimanje. Zlonamjerni kod bio je ugrađen u različite aplikacije, ali i u digitalne datoteke koje su žrtvama bile predstavljene kao ponude za visoko plaćene poslove. Tako su se, primjerice, s pojedinim žrtvama vodili intervjui za posao i testiranja, a sve u svrhu predstavljanja poslane datoteke sa štetnim kodom kao vjerodostojne ponude za posao. Aplikacije i ponude za posao promovirane su preko društvenih mreža i drugih komunikacijskih kanala.[55] Izravne žrtve napada bile su osobe uključene u postupak validiranja transakcija u mreži Ronin, koji su napadači namjeravali kompromitirati. Riječ je upravo o navedenim subjektima koji imaju kontrolu nad mrežom, ali i izravan interes u tome da održe funkcionalnost mreže i zaštite legitimnost transakcija. Ukupno je postojalo devet

[53] Washington, D.C., FBI National Press Office (202) 324-3691, Izvorno izvješće od 23. 1. 2023. „FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft", dostupno na https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft#Original-Statement (pristupljeno 15. srpnja 2025.).

[54] Ibid.

[55] Cybersecurity and Infrastructure Security Agency, „TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies", dostupno na: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a, (pristupljeno 15. srpnja 2025.) ; U.S. Department of the Treasury, Press Releases „U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats", dostupno na: https://home.treasury.gov/news/press-releases/jy0768 (pristupljeno 15. srpnja 2025.).

ovakvih subjekata s ulogom tzv. validatora, odnosno osoba zaduženih za provjeru i odobravanje transakcija.

Napadači su nakon stjecanja lozinki i podataka za prijavu, dobivenih socijalnim inženjeringom, preuzeli kontrolu nad četiri validatora mreže Ronin. Iskoristili su i ranije uspostavljenu, ali u međuvremenu zaboravljenu poveznicu između društva Sky Mavis i tzv. Axie DAO-a, decentralizirane autonomne organizacije povezane s istom aplikacijom te su, temeljem protupravno stečenih podataka iz tog prethodnog napada na Sky Mavis, ostvarili pristup i petom validatoru. Budući da je za ovjeru transakcija bilo potrebno odobrenje pet od ukupno devet validatora, napadači su time stekli kontrolu dostatnu da neometano odobre bilo koju transakciju te prenesu sredstva na digitalne novčanike pod vlastitom kontrolom.

Nakon uspješno provedenog kibernetičkog napada na mrežu Ronin, grupa Lazarus prenijela je sredstva putem različitih kanala na elektroničke novčanike pod svojom kontrolom. Ministarstvo financija SAD-a poduzelo je niz izvanrednih mjera kako bi spriječilo pranje i daljnji transfer ukradenih sredstava. Ključna taktika grupe sastojala se u korištenju usluge miješanja kriptovaluta Blender.io, putem koje je radi prikrivanja tragova transferirano više od 20,5 milijuna američkih dolara. Kao odgovor, Ured za kontrolu inozemne imovine (OFAC) prvi je put u povijesti sankcionirao pružatelja usluge miješanja kriptoimovine (tzv. kripto-mikser), odnosno usluge kojom se podrijetlo sredstava prikriva miješanjem kriptoimovine različitih imatelja kroz niz transakcija.[56] Predmetnom su pružatelju zamrznuta sva sredstva koja se nalaze pod američkom jurisdikcijom, a američkim je osobama zabranjeno daljnje poslovanje s njim. Uz to, OFAC je identificirao nove novčanike povezane s grupom Lazarus kako bi dodatno otežao raspolaganje sredstvima. Unatoč navedenim mjerama, veći dio ukradenih sredstava, u iznosu većem od 500 milijuna američkih dolara, ipak je premješten te potencijalno konvertiran putem decentraliziranih platformi i drugih nereguliranih kanala.

Naknadna forenzička analiza potvrdila je inicijalne navode te je ukazala na to da je kampanja dio šireg, kontinuiranog napora Demokratske Narodne Republike Koreje da generira prihode nezakonitim kibernetičkim aktivnostima, izbjegavajući time međunarodne sankcije. Osobito je značajno strateško usmjerenje prema sektorima koji se bave pohranom, konverzijom i špekulativnim trgovanjem digitalnom imovinom.[57] Budući da DNR Koreja ne surađuje s međunarodnom zajednicom te se već nalazi pod opsežnim režimom međunarodnih sankcija,[58] nezakonito stečena

[56] U.S. Department of the Treasury, Press Releases „U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats“, dostupno na: https://home.treasury.gov/news/press-releases/jy0768 (pristupljeno 15. srpnja 2025.). Sankcije su donesene na temelju izvršne uredbe (Executive Order) br. 13694, kako je izmijenjena izvršnom uredbom br. 13757.

[57] Washington, D.C., FBI National Press Office, Nadopunjeno izvješće od 6. 2. 2023., dostupno na: https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft#Original-Statement (pristupljeno 15. srpnja 2025.).

[58] Sankcijski režim prema Demokratskoj Narodnoj Republici Koreji uspostavljen je Rezolucijom Vijeća sigurnosti Ujedinjenih naroda br. 1718 (2006.), dostupno na: https://docs.un.org/en/S/RES/1718%20(2006) te je naknadnim rezolucijama postupno proširivan.

sredstva koja nisu pravodobno blokirana ostala su bespovratno pod kontrolom navedene kriminalne skupine.

3.2. Hakerski napadi na (kripto)infrastrukturu i softver za iznudu

Kibernetički napadi u sferi kriptoimovine mogu biti usmjereni i na fizičke uređaje smještene u razvijenim državama. Tako je primjerice u kolovozu 2022. godine proveden sofisticirani napad usmjeren na fizičku kripto-infrastrukturu u Republici Češkoj. U napadu na uređaje za isplatu gotovine u zamjenu za kriptoimovinu (tzv. kriptobankomate) društva General Bytes otuđena je kriptoimovina znatne vrijednosti u obliku Bitcoina i Ethera.

Napadači su iskoristili tzv. ranjivost nultog dana (engl. zero-day vulnerability)[59] u softverskom sustavu koji pokreće navedene kriptobankomate. Cilj napada bio je daljinski upad u sustav te preusmjeravanje transakcija krajnjih korisnika na novčanike pod kontrolom napadača. Tako bi osobe koje bi obavljale prijenos sredstava ili podizanje gotovine putem kriptobankomata, umjesto na elektronički novčanik namjeravanog primatelja, sredstva prenijele na elektronički novčanik pod kontrolom napadača.[60] Zločinačka je skupina društvu General Bytes u samome zlonamjernom kodu uputila zahtjev za plaćanje otkupnine kao uvjet za uklanjanje štetnog softvera i ponovno uredno funkcioniranje sustava. Međutim, oštećenik je, nakon što je utvrdio izvor problema, vlastitim tehničkim mjerama uspio otkloniti sigurnosni propust koji je napadačima omogućavao preusmjeravanje sredstava.[61]

Slučaj General Bytesa predstavlja kombinaciju izravnog napada na (kripto) infrastrukturu, otuđenja kriptoimovine i iznude. Slični se obrasci, međutim, pojavljuju i u brojnim drugim sektorima. Tako je cijeli niz industrija pogođen pokušajima iznude u kojima je korišten softver za iznudu.[62] Naime, softver za iznudu predstavlja specifičan oblik zlonamjernog računalnog programa (engl. *malware*) čija je osnovna funkcija neovlašteno ograničavanje pristupa računalnim podacima ili sustavima, najčešće putem šifriranja (kriptiranja), s ciljem iznude otkupnine od žrtve u zamjenu za ponovno omogućavanje pristupa tim podacima.[63] Sustav se blokira tako što netko nemarom instalira zaraženu datoteku, ili se zbog nedovoljnih sigurnosnih mehanizama počinitelji uspiju samostalno uključiti na sustav žrtava te instalirati štetni softver. Ovaj štetni softver onda se replicira unutar sustava kako bi

[59] Singh, U. K.; Chanchala, J.; Kanellopoulos, D., *A framework for zero-day vulnerabilities detection and prioritization,* Journal of Information Security and Applications 46 (2019.): 164-172, str. 164.

[60] „Security Incident August 18th 2022“, dostupno na: https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2785509377/Security+Incident+August+18th+2022, (pristupljeno 15. srpnja 2025.).

[61] „Security Incident August 18th 2022“, dostupno na: https://securityaffairs.com/134664/hacking/general-bytes-bitcoin-atm-zero-day.html (pristupljeno 15. srpnja 2025.); https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/954728558/Configuring+Server+Firewalls.

[62] U hrvatskom kaznenom pravu napadi softverom za iznudu u pravilu će ostvarivati obilježja kaznenih djela ometanja rada računalnog sustava (čl. 267. KZ-a) i oštećenja računalnih podataka (čl. 268. KZ-a), u stjecaju s iznudom (čl. 243. KZ-a), dok se izrada i stavljanje na raspolaganje takvog zlonamjernog softvera može kvalificirati kao zlouporaba naprava (čl. 272. KZ-a).

[63] O'Kane, P.; Sezer, S. & Carlin, D., *Evolution of ransomware*, Iet Networks, 2018., 7(5), 321-327.

u određenom trenutku blokirao sve datoteke u sustavu. Među najčešćim su žrtvama subjekti čije su usluge od šireg društvenog značaja, poput zračnih luka, bolnica i pružatelja IT usluga. Jedan od takvih napada dogodio se 2024. godine i u Republici Hrvatskoj, kada je žrtvom napada bila Zračna luka Split.[64]

Neovisno o tome je li napad usmjeren na fizičku infrastrukturu, na sustave izravno vezane uz kriptoimovinu ili na druge ciljeve, plaćanje otkupnine redovito će se zahtijevati upravo u različitim kriptovalutama, a za prikrivanje daljnjeg tijeka sredstava zločinačke će skupine koristiti metode slične onima prikazanima kod prethodno opisanih hakerskih napada. Najčešće će pritom biti riječ o tzv. *privacy coinovima*, odnosno kriptovalutama čije se transakcije zbog ugrađenih mehanizama zaštite privatnosti znatno teže mogu pratiti analizom blockchaina.[65]

4. MEĐUNARODNA BORBA PROTIV PRANJA NOVCA I FINANCIRANJA TERORIZMA

Suzbijanje financiranja terorizma i provedbe aktivnosti računalnog kriminaliteta zahtijeva pravni okvir koji je jednako adaptivan i transnacionalnog karaktera kao i navedene ilegalne aktivnosti. Zločinačke organizacije i terorističke skupine kontinuirano razvijaju nove metode izbjegavanja međunarodnog nadzora i kontrole.[66] Tako će upravo ovi akteri tražiti mehanizme zaobilaženja novih mjera za sprečavanje pranja novca i provedbe ilegalnih novčanih tokova. Sve veća razina međunarodne suradnje i globalna integracija financijskog sektora, međutim, otežavaju ovim skupinama nesmetano provođenje ilegalnih aktivnosti preko bankarskog sustava.[67] Nove financijske tehnologije, naročito one vezane uz kriptoimovinu, stoga predstavljaju novi alat za zločinačke organizacije.[68]

Na značaj međunarodne koordinacije u borbi protiv financiranja terorizma ukazuju i Ujedinjeni narodi pa tako 2005. donose rezoluciju Vijeća sigurnosti UN-a, koja stavlja naglasak na međunarodnu suradnju u tim pitanjima.[69] Rezolucijom

[64] Vlada Republike Hrvatske, „Hakerski napad na zračnu luku je slučaj ransomwarea“, dostupno na: https://vlada.gov.hr/vijesti/hakerski-napad-na-zracnu-luku-je-slucaj-ransomwarea/42774 (pristupljeno 16. srpnja 2025. godine).

[65] Kriptovalute usmjerene na zaštitu privatnosti (engl. *privacy coins*), poput Monera, primjenom dodatnih kriptografskih mehanizama prikrivaju podatke o pošiljatelju, primatelju i iznosu transakcije, zbog čega je njihovo praćenje metodama blockchain forenzike bitno otežano. Opširnije vidjeti: Dupuis, D.; Gleason, K., *Money laundering with cryptocurrency: open doors and the regulatory dialectic,* Journal of financial crime 28.1 (2021.), str. 60-74.

[66] Izvješće FATF-a ‘’*Comprehensive Update on Terrorist Financing Risks’’,* srpanj 2025., dostupno na: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025, 11. kolovoza 2025.

[67] Steblianko, A. V.; Chernadchuk, T. O.; Kravchenko, I. O.; Andriichenko, N. S.; Rudanetska, O. S., *International law enforcement cooperation against money laundering*, Cuestiones Politicas, Vol. 37, god. 65. str. 219.

[68] Za više vidi Collins J., *Crypto, crime and control, Cryptocurrencies as an enabler of organized crime*, Global Initiative Against Transnational Organized Crime, 2022.

[69] Rezolucija Vijeća sigurnosti Ujedinjenih naroda br. 1617 (2005.), dostupno na: https://docs.un.org/en/S/RES/1617%20(2005).

je prepoznat rad FATF-a u postavljanju standarda, koordinaciji i izgradnji kapaciteta koji predstavljaju model za paraliziranje financija terorističkih skupina i sprečavanje pranja novca. Međunarodna zajednica prepoznala je preporuke FATF-a kao međunarodne standarde u borbi protiv pranja novca i financiranja terorizma pa tako oni danas predstavljaju temelj za sve druge zakonodavne okvire država i supranacionalnih tijela.

4.1. FATF i preporuke za suzbijanje pranja novca i borbu protiv financiranja terorizma

FATF (Financial Action Task Force) osnovan je na summitu G7 u Parizu 1989. godine, kao odgovor na prijetnju koju je pranje novca predstavljalo za međunarodne i nacionalne financijske sustave.[70] Organizaciju je prvotno činilo šesnaest država te je imala početni zadatak proučiti tehnike i trendove pranja novca, pregledati nacionalne i međunarodne mjere koje su već poduzete te identificirati buduće korake za borbu protiv pranja novca. FATF je u tom smislu već u travnju 1990. godine predstavio Četrdeset preporuka o pranju novca.[71] Kako bi se išlo u korak s promjenama u obrascima kriminalnih aktivnosti, već 1996., a potom i 2003. godine tih četrdeset preporuka revidirano je i nadopunjeno te one danas čine međunarodni standard u borbi protiv pranja novca. Preporuke su vezane kako uz nacionalnu pravnu regulaciju tako i uz međunarodnu suradnju.

Nakon događaja od 11. rujna 2001., mandat FATF-a proširen je na suzbijanje financiranja terorizma, što je za posljedicu imalo donošenje Osam posebnih preporuka protiv financiranja terorizma u siječnju 2002. godine. Preporuke su proširene u listopadu 2004. na Devet posebnih preporuka.[72] Te posebne preporuke za sprečavanje financiranja terorizma uključuju: kriminalizaciju pranja novca i financiranja terorizma; davanje istražnim tijelima ovlasti za praćenje, zapljenu i konfiskaciju imovine stečene kaznenim djelima; uspostavu okvira za prekograničnu razmjenu informacija; proširenje zahtjeva AML-a na alternativne sustave prijenosa novca; i osiguranje da se neprofitne organizacije ne mogu zloupotrijebiti za financiranje terorizma. FATF 2012. godine revidira sve svoje dosadašnje preporuke u jedinstvenih 40 preporuka te upravo one predstavljaju jedinstveni sustav međunarodnog standarda u borbi protiv pranja novca i financiranja terorizma. [73]

Ključni aspekt preporuka FATF-a vezan je uz pristup KYC – ''know your client'' (poznaj svog klijenta). Taj pristup podrazumijeva ukidanje anonimnih računa, identifikaciju svih klijenata, čuvanje evidencije o transakcijama najmanje

[70] Vidjeti više, https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html, 7. kolovoza 2025.

[71] Petrović, T., *Inicijativa međunarodnih organizacija u prevenciji pranja novca i financiranja terorizma,* Pravnik: časopis za pravna i društvena pitanja, 55, br. 107 (2021.), str. 277.

[72] FATF, 9 Special Recommendations 2004., dostupno na: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Ixspecialrecommendations.html, 8. kolovoza 2025.

[73] FATF, The FATF Recommendations, dostupno na: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html, 7. kolovoza 2025.

pet godina, dostupnost svih evidencija pravosudnim tijelima na zahtjev te obavještavanje nadležnih tijela u slučaju neuobičajenih ili sumnjivih transakcija.[74] Također, FATF preporučuje državama da kriminaliziraju pranje novca kao i da daju tijelima vlasti pravnu moć za identifikaciju, praćenje i oduzimanje nezakonito stečenog novca. Pored navedenoga, u kontekstu ovoga rada valja izdvojiti i sljedeće ključne mehanizme sprečavanja pranja novca.

Dubinska analiza klijenta jedan je od tih ključnih mehanizama. Sadržana u Preporuci 10., zahtijeva od financijskih i nefinancijskih institucija da primjenjuju dubinsku analizu klijenta u vidu identifikacije klijenta i verifikacije njegova identiteta, pribavljanja informacija o svrsi i prirodi poslovnog odnosa, provođenja stalnog nadzora i ostalih mjera prilikom uspostavljanja pravnog odnosa, obavljanja povremenih transakcija iznad određenog praga ili u slučaju sumnje na pranje novca ili financiranje terorizma, bez obzira na iznos transakcije.[75]

Čuvanje podataka o transakcijama spada pod 11. preporuku FATF-a. U toj preporuci zahtijeva se između ostalog da financijske institucije moraju čuvati potrebne evidencije o transakcijama (uključujući originalne dokumente ili njihove kopije) najmanje pet godina, kako bi mogle brzo dostaviti te informacije nadležnim tijelima u svrhu prevencije pranja novca i financiranja terorizma.[76]

Nadalje, jedan od ključnih mehanizama u sprečavanju pranja novca i financiranja terorizma nalazi se u FATF-ovoj preporuci broj 15. pod nazivom Nove tehnologije. Prije svega, ova preporuka odnosi se na kriptosektor. Njome se preporučuje da zemlje trebaju osigurati da pružatelji usluga virtualne imovine (VASP) budu podvrgnuti mjerama za sprečavanje pranja novca i financiranja terorizma, uključujući njihovu registraciju ili licenciranje te podložnost nadzoru i provedbi mjera sukladnosti s ostalim FATF-ovim standardima, kao što su primjerice dubinska analiza klijenta (preporuka br. 10.), prijavljivanje sumnjivih transakcija (preporuka br. 20.), obveza da VASP-ovi prikupljaju i prenose podatke o pošiljatelju i primatelju (Preporuka br. 16. tzv. „Travel Rule“) i ostale.[77]

Upravo je preporuka 16., tzv. Travel Rule, jedan od ključnih mehanizama sprečavanja pranja novca, a odnosi se na transparentnost transakcija. Glavni je cilj spriječiti da teroristi i drugi kriminalci imaju neograničen pristup platnim sustavima za premještanje svojih sredstava, te omogućiti otkrivanje takve zlouporabe kada do nje dođe. Konkretno, cilj je osigurati da osnovni podaci o pošiljatelju i primatelju plaćanja ili prijenosa vrijednosti budu odmah dostupni tijelima nadležnima za otkrivanje sumnjivih transakcija.[78]

---

[74] Gardner, K. L., *Fighting terrorism the FATF way*, Global Governance, 13(3), str. 330.

[75] *Op. cit.* bilj. 64.

[76] Clavijo Suntura, J. H., *Customer Identification in Currency Exchange Companies as per FATF Recommendations,* Journal of Money Laundering Control, 23/1, str. 98.

[77] Pavlidis, G., *International Regulation of Virtual Assets under FATF's New Standards,* Journal of Investment Compliance 21/1 (2020.) str. 1-8.

[78] *Op. cit*. bilj. 64.

Uspostavljanje tih međunarodnih standarda postupanja tek je prvi korak u stvaranju učinkovitog sustava sprečavanja pranja novca i u borbi protiv financiranja terorizma. Jedna je od glavnih zadaća FATF-a i ujednačena i dosljedna primjena tih standarda širom međunarodne zajednice. Ako se standardi primjenjuju bez uniformnosti ili odgovarajuće strogosti, terorističke i zločinačke organizacije pronaći će mehanizam uključivanja u međunarodni financijski sustav kroz „najslabije karike", odnosno financijske sustave država koje provode nepotpune ili manje učinkovite provjere.[79]

FATF je iz tog razloga razvio specifične procese za procjenu pridržavanja preporuka u odnosu na države članice i države nečlanice.[80] Jedan od tih postupaka jest i NCCT (Non-Cooperative Countries and Territories). Taj postupak razvio je FATF s glavnim ciljem da identificira jurisdikcije koje su sustavno odbijale surađivati i uskladiti svoje pravne okvire s međunarodnima.[81] Zemlje koje su identificirane kao nesuradničke javno su osuđivane i podvrgnute međunarodnom pritisku te im je ograničen pristup financijskim tokovima.

Ovaj je mehanizam, u svojoj biti, djelovao kao instrument međunarodnopravne i financijske prisile, potičući subjekte na pravovremeno donošenje i implementaciju potrebnih zakonodavnih i institucionalnih reformi. S obzirom na njegovu učinkovitost u ranom razdoblju, većina jurisdikcija podvrgnutih postupku brzo je uskladila svoje sustave sa standardima FATF-a što je omogućilo postupno ukidanje formalnog NCCT-a, zamijenjena sustavom evaluacije i nadzora, koji uključuje dvostupanjski model.[82] Taj je model, s obzirom na stupanj suradnje i usklađenosti, zemlje svrstavao kao zemlje pod pojačanim nadzorom (tzv. „siva lista") i zemlje sa strateškim nedostacima (tzv. „crna lista").

4.2. FATF i kriptoimovina

Iako kriptoimovina ima cijeli niz legalnih primjena, pojedine ključne karakteristike kriptoimovine, poput decentralizacije sustava, idealne su upravo za aktivnosti kriminalnih organizacija.[83] Kao što je prethodno navedeno, upravo su mjere poput ukidanja anonimiziranih bankovnih računa ili nenadziranih transakcija bile od ključnog značaja za borbu protiv financiranja terorizma i pranja novca. Zato alternativni financijski tokovi putem kriptovaluta predstavljaju novi mehanizam za ilegalne novčane transakcije koji stoji u izravnome konfliktu s ciljevima FATF-a.

FATF je stoga bio i prva međunarodna organizacija koja je razvila strateški odgovor na sigurnosne rizike kriptovaluta. U usporedbi s nacionalnim regulatorima,

---

[79] Pavlidis, G., *Financial action task force and the fight against money laundering and the financing of terrorism: Quo vadimus?,* Journal of Financial Crime 28.3 (2021), str.765-773.

[80] *Op. cit*. bilj. 65. str. 332.

[81] Za više v. Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations, dostupno na: https://www.fatf-gafi.org/en/publications/Mutualevaluations/4th-round-procedures.html, 22. srpnja 2025.

[82] *Op. cit.* bilj. 65, str. 332.

[83] *Op. cit.* bilj. 58.

FATF je djelovao rano u procjeni značajnih rizika koje kriptovalute predstavljaju za režim sprečavanja pranja novca i financiranja terorizma. Tako već 2014. i 2015. godine FATF objavljuje analizu rizika i smjernice specifične za kriptovalute, dok je 2018. godine izmijenio svoje obvezne preporuke kako bi izričito primijenio svoja pravila na kriptovalute.[84]

Kako bi osigurao što veću učinkovitost propisa i spriječio zaobilaženje svojih globalnih Preporuka, FATF je dao široku definiciju kriptoimovine. Umjesto izraza „kriptovaluta" ili „digitalna imovina", FATF koristi termin „virtualna imovina" kako bi obuhvatio svaku digitalnu vrijednost kojom se može digitalno trgovati ili prenositi te se može koristiti za plaćanje ili ulaganje.[85] Kao što je uvodno navedeno, na ovaj način obuhvaćaju se ne samo decentralizirane, već i centralizirane virtualne vrijednosti.

Kao i kod reguliranja drugih financijskih aktivnosti, FATF je identificirao i iznimno široko definirao platforme za virtualnu imovinu koje su sposobne nadzirati financijske aktivnosti provedene putem njihovih sustava, tzv. „pružatelje usluga povezanih s virtualnom imovinom" (VASP).[86] Sve države moraju uspostaviti zahtjeve za licenciranje ili registraciju VASP-ova. VASP-ovi moraju biti licencirani u jurisdikcijama u kojima su pravno osnovani.[87] Pojedine države mogu dodatno zahtijevati licenciranje ili registraciju kao uvjet za obavljanje poslovanja. VASP-ovi bi trebali biti podložni cjelokupnom skupu preventivnih mjera i obveza iz područja suzbijanja pranja novca i financiranja terorizma, slično kao i drugi financijski posrednici.[88]

S obzirom na prekograničnu prirodu aktivnosti VASP-ova, Preporuke FATF-a zahtijevaju od njih primjenu dodatnih preventivnih mjera. U pogledu zahtjeva za dubinskom analizom stranke (Customer Due Diligence – CDD), propisanih Preporukom 10, FATF je 2019. godine uveo niski prag od 1000 američkih dolara / eura za transfere virtualne imovine (VA) koji aktiviraju obveze CDD-a.[89]

Nadalje, FATF je usvojio i tzv. „Travel Rule" koji se primjenjuje i na VASP-ove. Travel Rule predstavlja izmjenu Preporuke 16 FATF-a koja se odnosi na prijenose novčanih sredstava (wire transfers) i zahtijeva od VASP-ova da prikupe, čuvaju i prenose potrebne podatke o pošiljatelju i primatelju, odmah i na siguran način, prilikom izvršavanja transfera virtualne imovine.[90] Ovo su iste obveze koje imaju tradicionalni financijski posrednici kada razmjenjuju podatke o transakcijama putem SWIFT-a.

---

[84] Wagman, S., *Cryptocurrencies and national security: the case of money laundering and terrorism financing*, Harv. Nat'l Sec. J. 14 (2022.), str. 87-89.

[85] Anggriawn, R.; Susila, M. E., *Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendation,* Novum Jus, 18/2 (2024.), str. 266.

[86] Ibid.

[87] *Op. cit.* bilj. 64.

[88] *Op. cit.* bilj. 70.

[89] *Op. cit.* bilj. 64.

[90] Mekrop, E. S., *Anti-Money Laundering and Combating the Financing of Terrorism Compliance,* Journal of Money Laundering Control, 22/3, str. 455.

5. REGULATIVA EU-a VEZANA UZ AML/CFT

Europska unija započela je razvoj svog zakonodavnog okvira glede sprečavanja pranja novca i financiranja terorizma nakon terorističkih napada na Sjedinjene Američke Države 2001. Tada se posebna pozornost posvetila presretanju i sprečavanju financijskih tokova kojima se financiraju terorističke organizacije. Europska unija u ovome periodu započinje intenzivnije usklađivanje svojih propisa s međunarodnim standardima FATF-a pa je tako donesen cijeli niz mjera kojima se nastojalo implementirati FATF-ove preporuke. Prve direktive bile su prvenstveno usmjerene na bankarski sektor. Od banaka se zahtijevalo identificiranje klijenata, prijavljivanje sumnjivih transakcija te vođenje odgovarajuće dokumentacije.[91] Kasnije su se obveze proširile i na druge financijske institucije, a poseban izazov predstavljao je razvoj digitalne imovine i virtualnih valuta. Te nove financijske instrumente kriminalne organizacije vješto su koristile za pranje novca i financiranje terorizma iz razloga što tradicionalni sustav nadzora nije bio prilagođen decentraliziranim oblicima prijenosa vrijednosti, zbog čega su se pojavile nove mogućnosti prikrivanja identiteta i prijenosa sredstava. Iz navedenih razloga Unija je donijela niz uredbi i direktiva kojima je htjela ići u korak s razvojem financijskih instrumenata.

Direktiva (EU) 2015/849 Europskog parlamenta i Vijeća, poznata kao AMLD4 (Anti-Money Laundering Directive),[92] bila je jedna od prvih značajnih direktiva vezanih uz sprečavanje pranja novca i financiranja terorizma. U tom je razdoblju predstavljala ključni pravni instrument Europske unije u borbi protiv zlouporabe financijskog sustava u svrhe pranja novca i financiranja terorizma. Direktivom se uspostavlja sveobuhvatan i učinkovit pravni okvir kojim se države članice obvezuju prepoznati, razumjeti i ublažiti rizike povezane s pranjem novca i financiranjem terorizma te u svoja nacionalna zakonodavstva implementirati propisane mjere i standarde.[93] Direktiva implementira niz FATF-ovih preporuka, prepoznajući važnost međunarodne usklađenosti i suradnje u cilju sprečavanja pranja novca i financiranja terorizma. Tako npr. direktiva propisuje postupak dubinske analize klijenata, odnosno u kojim se okolnostima primjenjuje CDD i koje su mjere obuhvaćene CDD-om (implementacija Preporuke br. 10), postupak donošenja i sadržaj izvješća za procjenu rizika od pranja novca i financiranja terorizma, odredbe kojima se uspostavlja registar stvarnih vlasnika (implementacija Preporuka 24 i 25), čuvanje evidencije i statističkih podataka 5 godina (implementacija preporuke 11), kao i suradnja na nacionalnoj razini i na razini EU-a u svrhu sprečavanja pranja

[91] Vidi više: Direktiva 2001/97/EZ Europskog parlamenta i Vijeća od 4. prosinca 2001. o izmjeni Direktive Vijeća 91/308/EEZ o sprečavanju korištenja financijskog sustava u svrhu pranja novca, SL L 344, 28. 12. 2001.

[92] Direktiva (EU) 2015/849 Europskog parlamenta i Vijeća od 20. svibnja 2015. o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, o izmjeni Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2005/60/EZ Europskog parlamenta i Vijeća i Direktive Komisije 2006/70/EZ, SL L 141, 5. 6. 2015 (u nastavku AMLD4 ili Direktiva 2015/849).

[93] *Op. cit.* bilj. 62, str. 275.

novca i financiranja terorizma. Ovom direktivom kao obveznici, osim banaka i financijskih institucija, označuju se i odvjetnici, računovođe, revizori, posrednici u nekretninama, pružatelji usluga igara na sreću i ostali.

Pružatelji usluga razmjene virtualnih valuta, kao i pružatelji skrbničke usluge novčanika nisu imali nikakvu obvezu u okviru AMLD4 za identifikaciju sumnjivih aktivnosti. Stoga su terorističke skupine imale mogućnost prenositi novac u financijski sustav Unije ili unutar mreža virtualnih valuta prikrivanjem prijenosa ili iskorištavanjem razine anonimnosti na tim platformama.[94] Bilo je zato od ključne važnosti proširiti područje primjene Direktive (EU) 2015/849 kako bi se uključili pružatelji usluga razmjene virtualnih valuta i fiducijarnih valuta kao i pružatelji skrbničke usluge novčanika pa je donesena Direktiva 2018/843 poznatija kao AMLD5.[95] Ta Direktiva proširila je obveznike primjene AML/CFT obveza i na VASP-ove te time implementirala preporuku 15, uvrstila je i niz drugih mjera u svrhu sprečavanja pranja novca i financiranja terorizma, specifičnih za kriptoimovinu.

5.1. Uredba o tržištima kriptoimovine i sprečavanje pranja novca

Nadalje, posebno mjesto među novijim zakonodavnim aktima Europske unije zauzima Uredba o tržištima kriptoimovine (MiCA)[96] kojom je prvi put uspostavljen sveobuhvatan i jedinstven regulatorni okvir za tržište kriptoimovine na razini Europske unije. Uredbom MiCA uspostavljen je sveobuhvatan regulatorni okvir za tržište kriptoimovine pri čemu je njezin temeljni cilj zaštita potrošača i ulagatelja te osiguravanje sigurnog, transparentnog i uređenog tržišta kriptoimovine. Iako primarna svrha uredbe nije sprečavanje pranja novca i financiranja terorizma,[97] uredba je usvojila neke od FATF-ovih preporuka i ona zajedno s drugim uredbama, koje ćemo analizirati, čini jedinstvenu cjelinu EU-prava vezanih uz AML/CFT sustav. Tako se, na primjer, MiCA nadovezuje na FATF-ovu Preporuku 15, prema kojoj se pružatelji usluga povezanih s virtualnom imovinom (VASP) moraju pridržavati istih obveza kao i tradicionalne financijske institucije. FATF-ova 15. preporuka zahtijeva da države ili supranacionalne tvorevine unutar svog zakonodavstva obvežu VASP-ove da identificiraju, procijene i poduzmu učinkovite mjere za suzbijanje pranja novca i financiranja terorizma.

---

[94] Za više vidi: Van der Linden, T.; Shirazi, T., *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, Financial Innovation, vol. 9, br. 1, 2023., str. 1-30.

[95] Direktiva (EU) 2018/843 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive (EU) 2015/849 o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma i o izmjeni direktiva 2009/138/EZ i 2013/36/EU, SL L 156, 19. 6. 2018., str. 43-74 (dalje u tekstu: Direktiva (EU) 2018/843 ili AMLD5).

[96] Uredba (EU) 2023/1114 Europskog parlamenta i Vijeća od 31. svibnja 2023. o tržištima kriptoimovine te o izmjeni uredbi (EU) br. 1093/2010 i (EU) br. 1095/2010 i direktiva 2013/36/EU i (EU) 2019/1937, SL L 150, 9. 6. 2023., str. 40-205 (dalje u tekstu: MiCA).

[97] Ipak u uvodnim izjavama uredbe MiCA (16) stoji kako bi svaki zakonodavni akt koji se donese u području kriptoimovine trebao doprinijeti i cilju suzbijanja pranja novca i financiranja terorizma.

Tako su npr. Unutar uredbe MiCA propisani i zahtjevi za dubinskom analizom klijenta, praćenje transakcija i prijava sumnjivih aktivnosti, sve sukladno AMLD4 i FATF-ovim preporukama. U skladu s FATF-ovom Preporukom 15, MiCA zahtijeva i obveznu registraciju i licenciranje svih kripto-ponuđača i izdavatelja stablecoina u EU-u, nadzor nad njihovim upravljanjem, kapitalom i operacijama. Važnost pridržavanja propisa o sprečavanju pranja novca i financiranja terorizma od strane pružatelja kripto-usluga dodatno je osnažena Uredbom MiCA s obzirom na to da prema njezinim odredbama, propust u uspostavi učinkovitih sustava i aranžmana usklađenih s Direktivom (EU) 2015/849 može za posljedicu imati povlačenje, odnosno oduzimanje licence za rad.

Uz Uredbu MiCA, sastavni dio zakonodavnog okvira Europske unije za regulaciju kriptoimovine čini i Uredba (EU) 2023/1113,[98] koja je donesena istoga dana kao i MiCA Uredba te zajedno s njom predstavlja dio jedinstvenog zakonodavnog paketa usmjerenog na uređenje tržišta kriptoimovine i jačanje mjera za sprečavanje pranja novca i financiranja terorizma. Dok MiCA uređuje izdavanje i pružanje usluga povezanih s kriptoimovinom kao takvih, Uredba (EU) 2023/1113 u bitnome proširuje primjenu pravila o transparentnosti prijenosa novčanih sredstava, tzv. „travel rule", i na prijenose kriptoimovine. Time je ova Uredba, za razliku od MiCA-e koja je prvenstveno tržišno-regulatornog karaktera, propis čija je primarna svrha sprečavanje pranja novca i financiranja terorizma. Njome se od pružatelja usluga povezanih s kriptoimovinom zahtijeva da uz svaki prijenos kriptoimovine prikupljaju, čuvaju i prenose podatke o nalogodavcu i primatelju, čime se VASP-ovi izjednačavaju s tradicionalnim pružateljima platnih usluga u pogledu obveze praćenja transakcija. Uredba (EU) 2023/1113 time predstavlja izravnu implementaciju FATF-ine Preporuke 16 (Travel Rule) u pravu Europske unije za sektor kriptoimovine.[99] Donošenjem ove Uredbe zatvara se krug zakonodavnih mjera kojima Unija nastoji uspostaviti dosljedan i ujednačen pristup suzbijanju rizika pranja novca i financiranja terorizma povezanih s kriptoimovinom.

5.2. Potreba za reformom i donošenje jedinstvenog pravnog sustava AML/CFT u okviru Unije

Kao što je već istaknuto tijekom ovoga rada, jedan od temeljnih problema dosadašnjeg sustava sprečavanja pranja novca i financiranja terorizma u Europskoj uniji bila je fragmentacija pravnog okvira. Naime, dosadašnji sustav AML/CFT bio je uglavnom propisan direktivama koje državama članicama ostavljaju diskreciju u pogledu načina prenošenja njihova sadržaja u nacionalno zakonodavstvo i postavljaju tek cilj koji treba ostvariti. S druge, pak, strane, uredbe se izravno primjenjuju u svim državama članicama i ne zahtijevaju poseban akt kojim bi se ta

[98] Uredba (EU) 2023/1113 Europskog parlamenta i Vijeća od 31. svibnja 2023. o informacijama koje se prilažu prijenosima novčanih sredstava i određene kriptoimovine i o izmjeni Direktive (EU) 2015/849, SL L 150, 9. 6. 2023. (dalje u tekstu: Uredba (EU) 2023/1113).

[99] Vidjeti uvodne izjave Uredbe (EU) 2023/1113.

pravila implementirala u nacionalne sustave. Sustav koji se gotovo dva desetljeća temeljio na nizu prethodno spomenutih direktiva AML-a doveo je do znatnih razlika u opsegu, strogosti i tempu primjene pravila AML/CFT među državama članicama, što su kriminalne i terorističke skupine zlouporabljivale usmjeravajući svoje tokove sredstava prema jurisdikcijama sa slabijom implementacijom.[100]

Analizirajući prateći dokument Europske komisije,[101] koji je poslužio kao osnova za prijedlog reforme sustava AML/CFT, zaključuje se da je Europska komisija kao glavne nedostatke dotadašnjeg regulatornog okvira označila tri međusobno uvjetovana strukturalna problema. Prvo je nedosljedna primjena propisa o sprečavanju pranja novca i financiranja terorizma među obveznicima, zatim nedostatna učinkovitost nacionalnog nadzora te ograničena suradnja i koordinacija među financijsko-obavještajnim jedinicama. Navedene strukturne slabosti onemogućavale su dosljednu i ujednačenu provedbu europskog regulatornog okvira, istodobno otvarajući prostor za iskorištavanje razlika među nacionalnim sustavima.

Prvi problem odnosio se na različitu primjenu obveza od strane privatnog sektora, odnosno financijskih i nefinancijskih obveznika. Budući da su se pravila temeljila na direktivama koje su države članice prenosile u svoja nacionalna zakonodavstva, nastale su znatne razlike u provedbi dubinske analize stranaka (Customer Due Diligence), utvrđivanju stvarnog vlasnika, procjeni rizika te prijavljivanju sumnjivih transakcija.[102] Takva regulatorna fragmentacija stvarala je pravnu nesigurnost, povećavala troškove usklađivanja za subjekte koji posluju u više država članica te uzrokovala premještanje poslovanja u jurisdikcije s blažim pravilima ili manje učinkovitim nadzorom. Drugi problem odnosio se na neujednačenu kvalitetu nacionalnog nadzora nad provedbom propisa AML/CFT. Europska komisija utvrdila je značajne razlike u organizaciji, stručnim kapacitetima i resursima nacionalnih nadzornih tijela, zbog čega razina nadzora nije bila jednaka u svim državama članicama. Posljedica takvog sustava bila je neujednačena primjena europskog zakonodavstva i slabljenje ukupne učinkovitosti sustava sprečavanja pranja novca i financiranja terorizma. Treći problem odnosio se na ograničenu koordinaciju i razmjenu informacija između nacionalnih financijsko-obavještajnih jedinica (FIU – *Financial Intelligence Unit)*. Iako svaki FIU prikuplja i analizira prijave sumnjivih transakcija, među državama članicama postojale su znatne razlike u organizaciji, metodologiji rada i postupcima razmjene podataka. Osim toga, obveznici su često bili suočeni s nedostatkom povratnih informacija o kvaliteti svojih prijava, dok ni sami FIU-ovi nisu redovito dobivali podatke o tome jesu li njihove analize

[100] Vidi više u: Bures, O., *The New EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism: A Paradigm Shift in EU Efforts to Combat Terrorist Financing*? Studies in Conflict & Terrorism, 2025., str. 1-31.

[101] Europska komisija, Commission Staff Working Document – Impact Assessment accompanying the Anti-money laundering package, SWD(2021) 190 final, Bruxelles, 20. srpnja 2021., dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0190 (pristupljeno 2. 7. 2026.).

[102] *Ibid.*

rezultirale kaznenim istragama ili osuđujućim presudama. Time je bio otežan razvoj kvalitetnijih analitičkih metoda i učinkovitije međunarodne suradnje.[103]

Upravo je radi otklanjanja te fragmentacije i postizanja jedinstvene i izravno primjenjive strukture pravila AML/CFT, Europska unija 31. svibnja 2024. donijela Uredbu (EU) 2024/1624[104] (tzv. AMLR, Anti-Money Laundering Regulation). Za razliku od ranijih direktiva, AMLR sadrži izravno primjenjiva pravila o dubinskoj analizi stranke, stvarnom vlasništvu, pragovima za gotovinska plaćanja i obveznicima primjene propisa, čime se znatno smanjuje prostor za razlike u nacionalnoj implementaciji. Obveznici primjene AMLR-a izričito uključuju i pružatelje usluga povezanih s kriptoimovinom, čime se obveze AML/CFT za sektor kriptoimovine prvi put ujednačavaju na razini cijele Unije uredbom, a ne, kao do sada, direktivom koju je svaka država članica implementirala na svoj način.

Važno je naglasiti da AMLR djeluje komplementarno s Direktivom (EU) 2024/1640 (tzv. AMLD6),[105] što ukazuje na namjeru zakonodavca da se ne radi o odvojenim, već o međusobno usklađenim i funkcionalno povezanim propisima koji zajedno čine novi regulatorni okvir. Dok AMLR sadržava jedinstvena i izravno primjenjiva materijalnopravna pravila koja uređuju obveze obveznika, Direktiva (EU) 2024/1640 uređuje institucionalni i provedbeni okvir sustava sprečavanja pranja novca i financiranja terorizma. Njome se državama članicama propisuje obveza uspostave i organizacije nacionalnih nadzornih tijela, financijsko-obavještajnih jedinica, registara stvarnih vlasnika te mehanizama međusobne suradnje i razmjene informacija, uz zadržavanje određenog stupnja diskrecije u pogledu njihova institucionalnog ustroja.

Istodobno, Direktiva (EU) 2024/1640 izričito stavlja izvan snage Direktivu (EU) 2015/849 (AMLD4) zajedno s njezinim naknadnim izmjenama, uključujući Direktivu (EU) 2018/843 (AMLD5).[106] Slijedom toga, prestanak važenja dosadašnjeg direktivnog okvira nije posljedica stupanja na snagu AMLR-a, nego izričite zakonodavne odluke da se postojeći sustav zamijeni novim, međusobno usklađenim regulatornim modelom koji čine AMLR i AMLD6. Oba prethodno navedena instrumenta stupila su na snagu u srpnju 2024. godine, dok je 10. srpnja 2027. određen kao datum njihove pune primjene, odnosno krajnji rok za prenošenje Direktive (EU) 2024/1640 u nacionalna zakonodavstva država članica. Time je uspostavljen dvoslojni regulatorni model u kojem AMLR osigurava jedinstvenost materijalnopravnih pravila na razini cijele Europske unije, dok AMLD6 omogućuje

[103] Bures, *op. cit.* u bilj. 91.

[104] Uredba (EU) 2024/1624 Europskog parlamenta i Vijeća od 31. svibnja 2024. o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, SL L 2024/1624, 19. 6. 2024. (dalje u tekstu: AMLR ili Uredba (EU) 2024/1624).

[105] Direktiva (EU) 2024/1640 Europskog parlamenta i Vijeća od 31. svibnja 2024. o mehanizmima koje države članice trebaju uspostaviti radi sprečavanja korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, o izmjeni Direktive (EU) 2019/1937 te o izmjeni i stavljanju izvan snage Direktive (EU) 2015/849, SL L, 2024/1640, 19. 6. 2024. (dalje u tekstu AMLD6 ili Direktiva (EU) 2024/1640).

[106] Vidi uvodne izjave Direktive (EU) 2024/1640.

njihovu učinkovitu institucionalnu provedbu, uz zadržavanje nužne fleksibilnosti u organizaciji nacionalnih sustava.

Donošenje izravno primjenjive uredbe (AMLR) i prateće direktive (AMLD6) bilo je tek jedan dio reforme. Kao jedan od problema unutar sustava AML/CFT identificiran je nedostatak jedinstvenog nadzornog tijela na razini Unije koje bi osiguralo ujednačenu primjenu i nadzor nad provedbom pravila AML/CFT. Stoga je istoga dana, 31. svibnja 2024., usvojena i Uredba (EU) 2024/1620 o osnivanju Tijela za sprečavanje pranja novca i borbu protiv financiranja terorizma (Anti-Money Laundering Authority – AMLA).[107] Već u uvodnim izjavama ove Uredbe Europska unija izrijekom navodi kako postojeći mehanizmi nadzora, koji su prvenstveno organizirani na nacionalnoj razini, nisu osigurali dosljednu primjenu pravila o sprečavanju pranja novca i financiranja terorizma te kako su razlike u intenzitetu i kvaliteti nacionalnog nadzora omogućile akterima koji se bave pranjem novca i financiranjem terorizma da iskoriste najslabije karike u sustavu.[108] AMLA stoga predstavlja novu agenciju Europske unije čija je temeljna zadaća transformacija i ujednačavanje nadzora nad sprečavanjem pranja novca i financiranja terorizma na razini cijele Unije, i to kako izravnim nadzorom nad odabranim visokorizičnim financijskim subjektima (uključujući, po potrebi, najveće pružatelje usluga povezanih s kriptoimovinom), tako i koordinacijom i nadzorom rada nacionalnih nadzornih tijela u preostalim sektorima, uključujući i nacionalna tijela nadležna za nadzor VASP-ova. AMLA bi prema planiranoj dinamici uspostave ubrzo trebala preuzeti nadzorne ovlasti, čime se otvara novo, jedinstveno nadzorno težište u europskom sustavu borbe protiv pranja novca, uključujući i u segmentu kriptoimovine.[109]

Donošenjem Uredbe (EU) 2024/1624 (AMLR), Direktive (EU) 2024/1640 (AMLD6) te uspostavom Europskog tijela za sprečavanje pranja novca i financiranja terorizma (AMLA) Europska unija provela je najopsežniju reformu svojeg sustava AML/CFT od njegova uspostavljanja. Novim regulatornim okvirom nastoje se ukloniti nedostaci koji su obilježavali prethodni sustav, osobito regulatorna fragmentacija, neujednačena primjena pravila među državama članicama te nedostatna koordinacija nacionalnih nadzornih tijela i financijsko-obavještajnih jedinica. Uspostavom jedinstvenih materijalnopravnih pravila, uz istodobno jačanje institucionalnog i nadzornog okvira, stvoreni su preduvjeti za dosljedniju i učinkovitiju provedbu mjera sprečavanja pranja novca i financiranja terorizma na razini cijele Europske unije. Poseban značaj reforme ogleda se u činjenici da su jedinstvena pravila prvi put u cijelosti obuhvatila i sektor kriptoimovine, čime su u

[107] Uredba (EU) 2024/1620 Europskog parlamenta i Vijeća od 31. svibnja 2024. o uspostavi Autoriteta za sprečavanje pranja novca i suzbijanje financiranja terorizma te o izmjeni uredbi (EU) br. 1093/2010, 1094/2010 i 1095/2010, SL L 2024/1620, 19. 6. 2024. (dalje u tekstu: AMLA).

[108] Vidi uvodne izjave br. 1-3 Uredbe (EU) 2024/1620 (AMLA), u kojima se obrazlaže da postojeći institucionalni okvir nadzora nije bio dovoljno učinkovit niti ujednačen na razini Unije, te da je za rješavanje tog problema potrebno uspostaviti novo nadzorno tijelo. Više o AMLA-i dostupno na: https://www.amla.europa.eu/index_en (pristupljeno 25. srpnja 2025.).

[109] Više vidi u: Hock, B., *Governing Money Laundering as a Collective-Action Problem: The European Anti-Money Laundering Authority (AMLA)*, European Journal of Risk Regulation, 2026., str. 1-16.

velikoj mjeri uklonjene regulatorne razlike koje su prethodno predstavljale prostor za zlouporabe. Time je uspostavljen integrirani europski sustav AML/CFT koji bi, uz djelovanje AMLA-e, trebao osigurati višu razinu pravne sigurnosti, učinkovitiji nadzor i otporniji financijski sustav Unije.

6. ZAKLJUČCI VEZANI ZA NEDOSTATKE POSTOJEĆE REGULATIVE NA PRIMJERU TRANSFERA SREDSTAVA IZ EU-a

U tradicionalnom financijskom sustavu, ulaz u monetarne tokove odvija se isključivo putem formalnih institucija, odnosno banaka, brokera i drugih pravnih subjekata koji podliježu strogoj regulativi. Ove institucije imaju pravnu osobnost, fizičku adresu i regulatornu obvezu provođenja mjera dubinske analize stranke (CDD), što ih čini učinkovitim „gatekeeperima" sustava u skladu s Preporukom 10 FATF-a. Na taj način, financijski sustav ostaje zatvoren te je nadzorom tih gatekeepera moguće spriječiti anonimne i nekontrolirane tokove novca.

Nasuprot tome, sektor virtualne imovine, odnosno kriptoimovine, temelji se na bitno drugačijim načelima. Iako su FATF i Europska unija opsežno definirali tko se sve smatra pružateljem usluga povezanih s virtualnom imovinom (Virtual Asset Service Providers – VASP), uključujući mjenjačnice, burze i skrbnike digitalnih novčanika, velik dio transakcija u kripto okruženju i dalje se može odvijati potpuno decentralizirano, bez ikakvog oslanjanja na formalne entitete.[110]

Svaka osoba može samostalno generirati vlastiti digitalni novčanik i koristiti ga za primanje i slanje sredstava bez posrednika. U slučaju kada se novac želi koristiti u svrhe financiranja terorizma, prvi korak uključuje konverziju gotovine u kriptovalutu – putem registrirane mjenjačnice pod nadzorom (npr. u Uniji, gdje su takve usluge sada podložne pravilima uredbe MiCA i Uredbe o prijenosu sredstava), ili izvan službenog kanala kroz kriminalne mreže koje prihvaćaju gotovinu i u zamjenu šalju kripto (tzv. off-chain transakcije).

Nakon što se sredstva nalaze u kripto obliku, mogu se prenijeti putem centraliziranih platformi poput Binancea, gdje korisnički novčanik zapravo funkcionira kao skrbnički račun – što znači da tijela javne vlasti mogu izdati nalog za zamrzavanje ili blokiranje sredstava. Međutim, ako korisnik koristi decentralizirani sustav, tada se transfer odvija na blockchainu izravno između dviju adresa, bez ikakve mogućnosti poništavanja ili zaustavljanja transakcije.

U završnoj fazi, sredstva se moraju ili ponovno konvertirati u fiat valutu, ili iskoristiti za nabavu roba i usluga. Ako se konverzija odvija u zemlji koja poštuje preporuke FATF-a, VASP-ovi u toj zemlji imaju obvezu nadzora i mogu identificirati korisnika. No, ako se sredstva prenesu u tzv. odmetnute države ili zemlje s visokom

[110] Dupuis, D.; Gleason, K, *Money laundering with cryptocurrency: open doors and the regulatory dialectic,* Journal of financial crime 28.1 (2021.), str. 67.

razinom pravne nesigurnosti i slabe regulacije, tada ne postoji učinkovit nadzor niti mogućnost pravovremene intervencije. Povijesno se učinkovitim pokazalo isključivanje takvih država iz međunarodnih financijskih sustava, čime se sprečavao prijenos novca na račune u tim državama. Međutim, s pojavom kriptoimovine, decentralizirane transakcije više nije moguće nadzirati na jednak način kao prije. Zbog gubitka klasičnih mehanizama blokade sredstava, nužno je koncentrirati se na dva aspekta sprečavanja pranja novca i financiranja terorizma.

Prvi je način primjena strožih sankcija, razmjernih novim izazovima i bitno strožih od mjera koje je FATF predviđao za bankovne i druge tradicionalne financijske transfere. Naime, prethodno su postojale učinkovite mjere blokiranja u slučajevima kada pojedine države ne bi surađivale s međunarodnom zajednicom, jer bi se prijenos sredstava u te države značajno mogao otežati. Danas to s kriptoimovinom nije moguće pa bi jedino strože sankcije mogle potaknuti te subjekte na suradnju u borbi protiv ovih nezakonitih aktivnosti. Takve bi mjere trebale uključivati sankcioniranje pojedinačnih adresa digitalnih novčanika, kao i pružatelja usluga miješanja kriptoimovine, po uzoru na OFAC-ovo sankcioniranje servisa Blender.io analizirano u trećem poglavlju. Uz to, trebalo bi predvidjeti sekundarne sankcije prema burzama, posrednicima i drugim pružateljima usluga koji nastavljaju poslovati s označenim subjektima, čime bi im se ograničio pristup reguliranom financijskom i kriptoimovinskom sustavu. Prema jurisdikcijama uvrštenima na FATF-ovu crnu listu mogle bi se primjenjivati i pojačane protumjere iz Preporuke 19 FATF-a, uključujući intenzivniju dubinsku analizu, ograničavanje poslovnih odnosa i, u krajnjem slučaju, potpunu zabranu ili uvjetovanje transakcija povezanih s tim jurisdikcijama. Štoviše, zbog opasnosti od stvaranja paralelnog sustava (decentraliziranog) plaćanja, valja razmotriti i alternativne sankcije koje se ne tiču isključivo ograničavanja transakcija.

Drugi je način daljnji razvoj sustava za predviđanje rizika. Danas se sve više podataka može prikupljati, podaci sa samih blockchaina u većini su slučajeva javno dostupni, a metode strojnog učenja razvijaju se iznimno brzo. Primjenom novih metoda temeljenih na umjetnoj inteligenciji i procjeni rizika pojedinih transakcija, mogli bi se barem dijelom spriječiti tokovi sredstava s računa unutar sustava na decentralizirane račune. Primjeri poput prethodno obrađenog slučaja napada grupe Lazarus ukazuju na to da postoji značajan interes za preventivnim privremenim zaustavljanjem velikih neuobičajenih transakcija. Naime, i značajni interni zaštitni mehanizmi te podjela kontrole nad nekim sustavom u konačnici ne moraju nužno biti dostatni za zaštitu takvog sustava, već bi mnogo značajniji učinak moglo imati privremeno blokiranje sustava i upozoravanje nadležnih tijela, jer bi se isključivo na taj način mogli spriječiti odljevi sredstava iz centraliziranih u decentralizirane sustave.

LITERATURA

Knjige i znanstveni članci

1. Alam, O., *Understanding the economies of blockchain games: An empirical analysis of Axie Infinity*. Distributed Computing Group Computer Engineering and Networks Laboratory ETH Zürich, 2022., URL: https://pub.tik.ee.ethz.ch/students/2 (2022.).
2. Arslanian, H. (2022.), *Ethereum.* U: *The book of crypto: The complete guide to understanding bitcoin, cryptocurrencies and digital assets* (pp. 91-98). Cham: Springer International Publishing.
3. Doguet, J. J., *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 2013., Louisiana Law Review, vol. 73.
4. Dourado, E.; Brito, J., 2014., *Cryptocurrency.* U: *The New Palgrave Dictionary of Economics.*
5. Emmert, F., *The regulation of cryptocurrencies in the United States of America*. European Journal of Law Reform 25 (2023): 1-2.
6. Gikay, A. A., *Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union Law*, 2018., Journal of Law, Technology & the Internet, Vol. 9.
7. Jozipović, Š.; Perkušić, T.; Keršić, M. (2025.). *Digitalni euro i kriptovalute: Sličnosti i moguće analogije za pravnu regulaciju*, u: Perkušić, M.; Jozipović, Š.; Pečarić, M. (ur.), *Digitalni euro i bezgotovinsko plaćanje: pravna regulacija i utjecaj na financijski sustav*, Sveučilište u Splitu.
8. Leiponen, A.; Llewellyn, D. W. T.; Wang, Q., *The dApp economy: A new platform for distributed innovation?,* Innovation 24, no. 1 (2022.): 125-143.
9. Martin, J., *Lost on the Silk Road: Online drug distribution and the 'cryptomarket'*, 2014., Criminology & Criminal Justice 14, no. 3.
10. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.*
11. O'Kane, P.; Sezer, S. & Carlin, D., *Evolution of ransomware*. Iet Networks, 2018., 7(5), 321-327.
12. Perkušić, M., *The Legal Treatment of Smart Contracts under Croatian Law* // Zbornik radova Pravnog fakulteta u Splitu, 61 (2024.), 4; 473-497. doi: 10.31141/zrpfs.2024.61.154.473
13. Perkušić, M., *Pravo elektroničkog plaćanja*, 2020., Školska knjiga, Zagreb.
14. Pflaum, I.; Hateley, E., *A bit of a problem: National and extraterritorial regulation of virtual currency in the age of financial disintermediation*, 2014., Georgetown Journal of International Law, vol. 45
15. Pupolizio, I. (2022.). *From libra to diem. the pursuit of a global private currency*. Global Jurist, 22(2), 281-306.
16. Raeesi, R., *The silk road, bitcoins and the global prohibition regime on the international trade in illicit drugs: can this storm be weathered?,* 2015., Glendon Journal of International Studies 8, 1-2.

17. Riley, J., *The current status of cryptocurrency regulation in China and its effect around the world*. China and WTO Review 7.1 (2021.): 135-152.
18. Singh, U. K.; Chanchala, J.; Kanellopoulos, D., *A framework for zero-day vulnerabilities detection and prioritization.* Journal of Information Security and Applications 46 (2019.): 164-172.
19. Taherdoost, H. (2022.). *Non-fungible tokens (NFT): A systematic review*. Information, 14(1), 26.
20. Tikhomirov, S. (2017, October). *Ethereum: state of knowledge and research perspectives*. In: International symposium on foundations and practice of security (pp. 206-221). Cham: Springer International Publishing.
21. Vuletić, D., *Pravna priroda kriptoimovine u pravu Europske unije i hrvatskom pravu*. Zbornik radova Pravnog fakulteta u Tuzli 10.1 (2024.): 67-94.
22. Wang, Q.; Li, R.; Wang, Q. & Chen, S. (2021.). *Non-fungible token (NFT): Overview, evaluation, opportunities and challenges*. arXiv preprint arXiv:2105.07447
23. Steblianko, A. V.; Chernadchuk, T. O.; Kravchenko, I. O.; Andriichenko, N. S.; Rudanetska, O. S., *International law enforcement cooperation against money laundering*, Cuestiones Politicas, Vol. 37, god. 65. str. 217-229.
24. Collins J., *Crypto, crime and control, Cryptocurrencies as an enabler of organized crime,* Global Initiative Against Transnational Organized Crime, 2022.
25. Petrović, T., *Inicijativa međunarodnih organizacija u prevenciji pranja novca i financiranja terorizma*, Pravnik: časopis za pravna i društvena pitanja, 55(107), str. 269-281.
26. Gardner, K. L., *Fighting terrorism the FATF way*, Global Governance, 13(3), str. 325-425.
27. Clavijo Suntura, J. H., *Customer Identification in Currency Exchange Companies as per FATF Recommendations,* Journal of Money Laundering Control, 23/1, str. 96-102.
28. O'Reilly, K. P. (2007.). *Perceiving Rogue States: The Use of the 'Rogue State' Concept by U.S. Foreign Policy Elites*. Foreign Policy Analysis.
29. Pavlidis, G., *International Regulation of Virtual Assets under FATF's New Standards,* Journal of Investment Compliance 21/1 (2020.) str. 1-8.
30. Pavlidis, G., *Financial action task force and the fight against money laundering and the financing of terrorism: Quo vadimus?,* Journal of Financial Crime 28.3 (2021), str. 765-773.
31. Wagman, S., *Cryptocurrencies and national security: the case of money laundering and terrorism financing*, Harv. Nat'l Sec. J. 14 (2022), str. 87-89.
32. Anggriawn, R.; Susila, M. E., *Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendation,* Novum Jus, 18/2 (2024.), str. 250-277.
33. Mekrop, E. S., *Anti-Money Laundering and Combating the Financing of Terrorism Compliance,* Journal of Money Laundering Control, 22/3, str. 451-471.

34. Dupuis, D.; Gleason, K., *Money laundering with cryptocurrency: open doors and the regulatory dialectic*, Journal of financial crime 28.1 (2021.), str. 60-74.
35. Hock, B., *Governing Money Laundering as a Collective-Action Problem: The European Anti-Money Laundering Authority (AMLA)*, European Journal of Risk Regulation, 2026., str. 1-16.
36. Bures, O., *The New EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism: A Paradigm Shift in EU Efforts to Combat Terrorist Financing*? Studies in Conflict & Terrorism, 2025., str. 1-31.
37. Van der Linden, T.; Shirazi, T., *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, Financial Innovation, vol. 9, br. 1, 2023., str. 1-30.
38. Wang, Z.; Sun, L. i Zhu, H. (2020.). *Defining Social Engineering in Cybersecurity.* IEEE Access, 8, 85094–85115.

Pravni akti

1. Protokol br. 1 uz Konvenciju za zaštitu ljudskih prava i temeljnih sloboda, Pariz, 20. ožujka 1952., ETS br. 009, stupio na snagu 18. svibnja 1954.
2. Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištima financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU.
3. Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija.
4. Direktiva (EU) 2019/2161 Europskog parlamenta i Vijeća od 27. studenoga 2019. o izmjeni Direktive Vijeća 93/13/EEZ i direktiva 98/6/EZ, 2005/29/EZ te 2011/83/EU Europskog parlamenta i Vijeća u pogledu boljeg izvršavanja i modernizacije pravila Unije o zaštiti potrošača.
5. Ustav RH, NN 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.
6. Uredba (EU) 2023/2854 Europskog parlamenta i Vijeća od 13. prosinca 2023. o usklađenim pravilima za pravedan pristup podacima i njihovu uporabu i o izmjeni Uredbe (EU) 2017/2394 i Direktive (EU) 2020/1828 (2023/2854, 22. 12. 2023).
7. Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (27. 12. 2022., L 333/1).
8. Uredba (EU) 2019/2088 Europskog parlamenta i Vijeća od 27. studenoga 2019. o objavljivanju informacija povezanih s održivošću u sektoru financijskih usluga, Uredba (EU) 2023/988 Europskog parlamenta i Vijeća od 10. svibnja 2023. o općoj sigurnosti proizvoda, izmjeni Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća i Direktive (EU) 2020/1828 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2001/95/EZ Europskog parlamenta i Vijeća i Direktive Vijeća 87/357/EEZ.

9. Uredba (EU) 2014/910 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ.
10. Direktiva (EU) 2023/2673 Europskog parlamenta i Vijeća od 22. studenoga 2023. o izmjeni Direktive 2011/83/EU u pogledu ugovora o financijskim uslugama sklopljenih na daljinu te o stavljanju izvan snage Direktive 2002/65/EZ; Direktiva 2015/2366/EU Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu.
11. Uredba (EU) 2023/1114 Europskog parlamenta i Vijeća od 31. svibnja 2023. o tržištima kriptoimovine te izmjeni uredbi (EU) br. 1093/2010 i (EU) br. 1095/2010 i direktiva 2013/36/EU i (EU) 2019/1937.
12. Zakon o provedbi Uredbe (EU) 2023/1114 o tržištima kriptoimovine (NN 85/24).
13. Uredba (EU) 2024/1620 Europskog parlamenta i Vijeća od 31. svibnja 2024. o uspostavi Autoriteta za sprečavanje pranja novca i suzbijanje financiranja terorizma te o izmjeni uredbi (EU) br. 1093/2010, 1094/2010 i 1095/2010, SL L 2024/1620, 19. 6. 2024.
14. Direktiva (EU) 2015/849 Europskog parlamenta i Vijeća od 20. svibnja 2015. o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, kojom se mijenja Uredba (EU) br. 648/2012 i ukidaju Direktiva 2005/60/EZ i Komisijska direktiva 2006/70/EC, SL L 141, 5. 6. 2015., str. 73-117.
15. Direktiva (EU) 2018/843 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive (EU) 2015/849 o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma i o izmjeni direktiva 2009/138/EZ i 2013/36/EU, SL L 156, 19. 6. 2018., str. 43-74.
16. Direktiva 2001/97/EZ Europskog parlamenta i Vijeća od 4. prosinca 2001. o izmjeni Direktive Vijeća 91/308/EEZ o sprječavanju korištenja financijskog sustava u svrhu pranja novca, SL L 344, 28. 12. 2001
17. Uredba (EU) 2024/1624 Europskog parlamenta i Vijeća od 31. svibnja 2024. o sprječavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, SL L 2024/1624, 19. 6. 2024.
18. Direktiva (EU) 2024/1640 Europskog parlamenta i Vijeća od 31. svibnja 2024. o mehanizmima koje države članice trebaju uspostaviti radi sprečavanja korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, o izmjeni Direktive (EU) 2019/1937 te o izmjeni i stavljanju izvan snage Direktive (EU) 2015/849, SL L, 2024/1640, 19. 6. 2024.

Ostali izvori

1. Washington, D.C., FBI National Press Office (202) 324-3691, Izvorno izvješće od 23. 1. 2023. „FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft", dostupno na https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft#Original-Statement (pristupljeno 15. srpnja 2025.).

2. Washington, D.C., FBI National Press Office, Nadopunjeno izvješće od 6. 2. 2023., dostupno na: https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft#Original-Statement (pristupljeno 15. srpnja 2025.).
3. Cybersecurity and Infrastructure Security Agency, „TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies“, dostupno na: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a, (pristupljeno 15. srpnja 2025.).
4. DAI (MakerDAO) dostupno na: https://makerdao.com/en/ (pristupljeno 25. srpnja 2025.).
5. EUROe, dostupno na: https://www.euroe.com/ (pristupljeno 25. srpnja 2025.).
6. „Security Incident August 18th 2022“ Dostupno na: https://securityaffairs.com/134664/hacking/general-bytes-bitcoin-atm-zero-day.html (pristupljeno 15. srpnja 2025.).
7. „Security Incident August 18th 2022“. Dostupno na: https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2785509377/Security+Incident+August+18th+2022, (pristupljeno 15. srpnja 2025.).
8. sUSD (Synthetix), dostupno na: https://www.synthetix.io/ (pristupljeno 25. srpnja 2025.).
9. Tether Gold (XAUT), dostupno na: https://gold.tether.to/ (pristupljeno 25. srpnja 2025.).
10. U.S. Department of the Treasury, Press Releases „U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats“, dostupno na: https://home.treasury.gov/news/press-releases/jy0768 (pristupljeno 15. srpnja 2025.).
11. Vlada Republike Hrvatske, „Hakerski napad na zračnu luku je slučaj ransomwarea“, dostupno na: https://vlada.gov.hr/vijesti/hakerski-napad-na-zracnu-luku-je-slucaj-ransomwarea/42774 (pristupljeno 16. srpnja 2025. godine).
12. Izvješće FATF-a „*Comprehensive Update on Terrorist Financing Risks“,* srpanj 2025., dostupno na: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.
13. FATF, 9 posebnih preporuka za sprječavanje financiranja terorizma, 2004., dostupno na: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Ixspecialrecommendations.html.
14. FATF, The FATF Recommendations, dostupno na: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.
15. Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations, dostupno na: https://www.fatf-gafi.org/en/publications/Mutualevaluations/4th-round-procedures.html, 22. srpnja 2025.

THE LEGAL STATUS OF VIRTUAL CURRENCIES IN INTERNATIONAL HACKING ATTACKS THAT FINANCE TERRORIST ACTIVITIES AND ROGUE STATES

The paper addresses the global challenges of regulating crypto-assets, with a focus on combating cybercrime and illicit financial activities. Since Bitcoin's emergence in 2008, the crypto-asset market has expanded rapidly, drawing increasing interest from individuals, businesses and institutional investors. While most crypto activity is legitimate, the decentralized and pseudonymous nature of these assets makes them appealing for illicit purposes such as money laundering, fraud, extortion, and terrorist financing. Despite progress in regulatory efforts, effective enforcement remains difficult without strong international cooperation.

The paper argues that existing regulation is insufficient given the borderless nature of crypto transactions. It explores how criminal groups acquire and use crypto-assets through cyberattacks, social engineering, and other digital crimes. Based on this, it emphasizes the difficulties faced by the global community in tracking illegal activities, particularly in regions with weak governance or countries with hostile regimes. In this context it examines the existing international legal framework, with particular focus on anti-money laundering (AML) and counter-terrorism financing measures. Based on this analysis, the paper underscores the urgent need for more cohesive and coordinated international regulatory strategies.

Key words: *AML, Anti-Money Laundering, Cryptocurrency, Crypto-asset, cybercrime*

© 2026 Zbornik radova Pravnog fakulteta u Splitu / *Collected Papers of the Faculty of Law in Split*.
Ovo je djelo licencirano pod licencom Creative Commons Imenovanje-Nekomercijalno-Bez prerada 4.0 međunarodna (CC BY-NC-ND 4.0) / *This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).*