

Zloupotreba digitalne imovine u prodaji falsifikovane robe u elektronskoj trgovini

Autorka: mr Andrea Mićanović
Januar 2026. godine



APSTRAKT

Razvoj digitalne ekonomije i elektronske trgovine otvorio je vrata novim mogućnostima za poslovanje, ali i novim oblicima zloupotreba, među kojima se posebno ističe prodaja falsifikovane robe. S tim u vezi, rad analizira ulogu digitalne imovine u olakšavanju i prikrivanju prometa falsifikovane robe na internetu. Poseban akcenat stavljen je na tehničke karakteristike digitalne imovine kao što su pseudoanonimnost, decentralizovanost, globalni domet, nepovratnost transakcija i proces tokenizacije. Oni doprinose stvaranju pravne nesigurnosti i otežavaju otkrivanje nezakonitih aktivnosti u okviru transakcija digitalnom imovinom. Naročito se ukazuje na pravne rizike povezane s upotrebom nezamjenjivih i imovinskih tokena u svrhu stvaranja privida autentičnosti falsifikovane robe. Na kraju, opšta preporuka je da se uspostavi sveobuhvatni regulatorni i nadzorni okvir koji bi omogućio efikasniju kontrolu tržišta digitalne imovine, uz očuvanje inovativnog potencijala *blockchain* tehnologije.

Ključne riječi:

digitalna imovina, kriptovalute, tokenizacija, nezamjenjivi tokeni, elektronska trgovina, falsifikovana roba, *blockchain* tehnologija, intelektualna svojina, regulacija tržišta.

Brza ekspanzija elektronske trgovine, podstaknuta imperativom globalizacije tržišta, donijela je istovremeno nove mogućnosti i izazove. Među izazovima se posebno izdvaja nagli porast prometa falsifikovane robe, koja je u digitalnom okruženju postala lako i globalno dostupna. Tom trendu posebno su doprinijeli razvoj i široka rasprostranjenost digitalne imovine koja, osim što funkcioniše kao sredstvo plaćanja u digitalnom prostoru, omogućava i prikrivanje porijekla sredstava, identiteta učesnika u transakcijama i autentičnosti same robe. Razlog za to je prije svega nepostojanje tradicionalnih mehanizama kontrole, što prodavcima i kupcima omogućava realizaciju transakcija koje nisu podložne neposrednoj intervenciji nadležnih tijela.

Stoga, cilj rada je da analitički prikaže na koji način karakteristike digitalne imovine utiču na širenje i funkcionalnost tržišta falsifikovane robe u elektronskoj trgovini, da identifikuje ključne pravne i institucionalne praznine koje omogućavaju ove zloupotrebe, te da ponudi praktične preporuke za unapređenje regulatornog i nadzornog okvira. Poseban akcenat je na procesu tokenizacije, koji predstavlja novi mehanizam kreiranja privida autentičnosti na digitalnom tržištu. Ideja je i da se odgovori na pitanje na koji način se norme o sprečavanju pranja novca (uključujući tzv. *Travel Rule*) mogu suprotstaviti izazovima koje pred regulatore postavljaju decentralizovani sistemi za razmjenu i plaćanje digitalnom imovinom.

Rad je strukturiran tako da prvo razjasni pojam i klasifikaciju digitalne imovine, zatim detaljno analizira mehanizme njene zloupotrebe u kontekstu elektronske trgovine, te konačno nudi preporuke usmjerene ka smanjenju rizika, uz nastojanje da se očuva inovativni potencijal *blockchain* tehnologije.

1. POJAM DIGITALNE IMOVINE

Mada razumijevanje pitanja digitalne imovine još uvijek nije u potpunosti ujedinilo naučnu i stručnu javnost, postoji nekoliko ključnih karakteristika koje je određuju. Prvo, riječ je o nematerijalnoj imovini koja postoji u digitalnom obliku, tj. označava digitalni zapis vrijednosti. Drugo, digitalna imovina može se elektronski prenositi i čuvati, što znači da su njeno postojanje i vlasništvo nad njom zabilježeni u formi elektronskog zapisa. Posredstvom elektronske mreže može se prenijeti sa jednog vlasnika na drugog uz istovremeni upis promjene vlasništva u relevantnom digitalnom registru ili sistemu zapisa.

Treće, digitalna imovina u tehničkom smislu zavisi od digitalnih tehnologija, tj. ne postoji izvan digitalnih sistema, pa se može reći da njeno postojanje, prenos i čuvanje omogućavaju informacione i komunikacione tehnologije. Takođe, za pojedine oblike digitalne imovine, a naročito za kriptoimovinu, karakteristična je upotreba kriptografije – tehnike šifrovanja podataka. Cilj šifriranja je “sigurna komunikacija preko nesigurnog komunikacijskog kanala”^[1] i ono predstavlja “način obezbjeđivanja sigurnosti transakcija, kontrole stvaranja dodatnih novčanih jedinica i potvrde transfera valute”^[2]. Pored kriptografije, za digitalnu imovinu od ključnog značaja je i *blockchain* tehnologija, odnosno tehnologija distribuiranog zapisa (eng. *distributed ledger technology* – *DLT*). Ona funkcioniše po principu decentralizovane i kriptografski osigurane digitalne knjige zapisa, “zasnovane na matematičkom algoritmu za distribuiranje kriptografskih informacija”^[3], koja omogućava transparentno, trajno i verifikovano bilježenje izvršenih transakcija, bez potrebe za centralnim posrednikom. Njen cilj je da riješi problem dvostrukog trošenja^[4], koji je sve do pojave bitcoina 2008. godine onemogućavao širu upotrebu digitalnih valuta.^[5]

I na kraju, digitalna imovina ima realnu ekonomsku vrijednost i može biti predmet pravnog prometa. Drugim riječima, može se koristiti kao sredstvo

razmjene, ulaganja, dokazivanja određenog prava ili plaćanja. Međutim, dok valuta kao zakonski priznato sredstvo plaćanja svoju vrijednost crpi iz autoriteta emitenta i zaštite države, virtualne valute nisu zakonska sredstva plaćanja^[6], nisu u širokoj upotrebi i njihova razmjena odvija se na osnovu sporazuma kupca i prodavca, koji ih prihvataju kao sredstvo plaćanja^[7]. Dakle, država nema punu monetarnu i regulatornu kontrolu nad tržištem digitalne imovine, čak ni kada se ona, u skladu sa voljom ugovornih strana, koristi kao sredstvo plaćanja u konkretnim transakcijama. To znači da su učesnici transakcije sa jedne strane pod velom državne zaštite ograničenog doseg^[8] a sa druge im je omogućeno da na različite načine zloupotrebljavaju digitalnu imovinu, pa i u svrhu prometa falsifikovane robe.

U skladu sa svim navedenim, čini se kao najsmislenije da se za potrebe ovog rada držimo definicije^[9] digitalne imovine koja je sadržana u srbijanskom Zakonu o digitalnoj imovini koja glasi:

Digitalna imovina označava digitalni zapis vrednosti koji se može digitalno kupovati, prodavati, razmenjivati ili prenositi i koji se može koristiti kao sredstvo razmene ili u svrhu ulaganja, pri čemu digitalna imovina ne uključuje digitalne zapise valuta koje su zakonsko sredstvo plaćanja i drugu finansijsku imovinu koja je uređena drugim zakonima.^[10]

^[1] Bagić, K. (2018). Kriptogram – vrlo kratak uvod. *Croatica*, 42 (62), 343-364. Dostupno na: <https://doi.org/10.17234/Croatica>.

^[2] Zimonja, O. i Vujić, D. (2020.) Kriptovalute – Izazovi aktuelnog globalnog trenda za kriminalističku praksu. *Kriminalistička teorija i praksa*, 7(2/2020), 55-71. Dostupno na: <https://hrcak.srce.hr/252827>.

^[3] Budimir, N. (2020). Blockchain tehnologija u osiguranju. *Elektronički zbornik radova Veleučilišta u Šibeniku*, 14 (1-2), 171-181. Dostupno na: <https://hrcak.srce.hr/241621>.

^[4] Dvostruko trošenje podrazumijeva trošenje jedne iste jedinice digitalne valute više od jednom zbog mogućnosti elektronskog kopiranja digitalnih zapisa koji sadrže njenu vrijednost i sve do početka primjene blockchain tehnologije, nepostojanja odgovarajućeg mehanizama sistemske kontrole.

^[5] Vidi: Cumming, D. J., Johan, S. i Pant, A. (2019.) Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty. *Journal of Risk and Financial Management*, 12(3), 126. Dostupno na: <https://doi.org/10.3390/jrfm12030126>.

^[6] Iz ovoga, argumentum a contrario, prozilazi da digitalna imovina ne obuhvata digitalne zapise valuta koje su zakonsko sredstvo plaćanja i drugu finansijsku imovinu.

^[7] Jovanić, T. (2021). Kriptovalute kao novi izazov zaštite potrošača. *Zbornik radova Pravnog fakulteta Univerziteta u Beogradu*, str. 396–427. Dostupno na: <https://plus.cobiss.net/cobiss/sr/sr/bib/39936009>.

^[8] Iako digitalna imovina ne predstavlja zakonsko sredstvo plaćanja, država može posredovati u sporovima koji nastanu povodom transakcija u kojima se ona koristi, na način što sudovi ne tretiraju digitalnu imovinu kao novac u smislu monetarnog prava već kao predmet pravnog odnosa koji je sredstvo plaćanja na osnovu ugovorne volje stranaka u kom slučaju će se primjenjivati opšta pravila obligacionog, privrednog, krivičnog prava... Ipak, s obzirom na to da država ne garantuje njenu vrijednost niti učestvuje u procesu plaćanja u digitalnoj valuti, zaštita učesnika u takvim transakcijama ostaje ograničena.

^[9] Ova definicija usaglašena je sa Direktivom EU br. 2018/843 od 30. maja 2018. godine o izmjeni Direktive EU br. 2015/849 o sprječavanju korišćenja finansijskog sistema u svrhu pranja novca i finansiranja terorizma i o izmjeni direktiva br. 2009/138/EZ i 2013/36/EU. Dostupna na: <https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng>.

^[10] Član 2 stav 1 tačka 1 Zakona o digitalnoj imovini ("Službeni glasnik Republike Srbije", br. 153/2020). Dostupan na: <https://www.paragraf.rs/propisi/zakon-o-digitalnoj-imovini.html>.

1.1. VRSTE DIGITALNE IMOVINE

Ako se zadržimo na prethodno citiranom propisu, digitalnu imovinu možemo podijeliti na virtuelne valute i digitalne tokene. Ove prve zakon definiše kao vrstu digitalne imovine koju nije izdala i za čiju vrijednost ne garantuje centralna banka, niti drugi organ javne vlasti, koja nije nužno vezana za zakonsko sredstvo plaćanja i nema pravni status novca ili valute ali je fizička ili pravna lica prihvataju kao sredstvo razmjene i može se kupovati, prodavati, razmjenjivati, prenositi i čuvati elektronski^[1]. Sa druge strane, digitalni tokeni predstavljaju bilo koje nematerijalno imovinsko pravo koje u digitalnoj formi predstavlja jedno ili više drugih imovinskih prava, što može uključivati i pravo korisnika digitalnog tokena da mu budu pružene određene usluge^[2].

Iako ne postoji univerzalna definicija virtuelnih valuta, one ipak imaju opšteprihvaćenu karakteristiku: virtuelna valuta nije fiducijarna valuta i ne bi je trebalo miješati s elektronskim novcem^[3]. Kriptovalute su vrsta virtuelnih valuta (iako se često koriste kao sinonimi) koje su kriptografski zaštićene i postoje na decentralizovanim platformama koje funkcionišu po principu *blockchain* tehnologije. U zavisnosti od namjene i funkcionalnosti, one se dalje dijele na novčiće i tokene – novčići su vezani za sopstveni *blockchain*, a tokeni se emituju na već postojećem. Primjera radi, Ether (ETH) je izvorni novčić *blockchaina* koji funkcioniše kroz Ethereum mrežu, dok je USDT ili Tether token koji nema sopstveni *blockchain*, već se emituje na više decentralizovanih *blockchain* platformi, uključujući Ethereum.

Teorija i praksa prepoznaju više vrsta digitalnih tokena, koje su uspostavljene u odnosu na različite kriterijume. Određene taksonomije zasnivaju se na funkcionalnim kriterijumima – razmatraju funkcije koje tokeni obavljaju i na osnovu toga uspostavljaju osnovne razlike među njima.

Prema njima, postoje tri vrste tokena, i to:

1. Platni tokeni (eng. *payment tokens*),
2. Uslužni tokeni (eng. *utility tokens*),
3. Sigurnosni tokeni (eng. *security tokens*).^[4]

Platni tokeni namijenjeni su upotrebi kao sredstvo plaćanja za dobra ili usluge izvan platforme na kojoj su izdati, tj. ugovorne strane ih prihvataju kao sredstvo za izmirenje međusobnih obaveza^[5], zamjenjujući funkciju novca i(li) razmjene vrijednosti^[6]. Primjera radi, USDT ili Tether je platni token koji funkcionira na više decentralizovanih *blockchain* platformi (Ethereum, Tron itd) i služi kao prilično rasprostranjeno sredstvo za obavljanje transakcija u okviru digitalnog tržišta, s obzirom na to da je njegova vrijednost vezana za američki dolar, pa nije podložna velikim tržišnim oscilacijama.

Prema Uredbi Evropske unije br. 2023/1114 o tržištima kriptovaluta (MiCA), uslužni token predstavlja vrstu digitalne imovine koja je namijenjena isključivo obezbjeđivanju pristupa određenom dobru ili usluzi koju pruža njen izdavalac^[7] posredstvom već uspostavljene *blockchain* infrastrukture, pri čemu se izdavaocem smatra fizičko ili pravno lice koje emituje kriptovalutu. Drugim riječima, uslužni tokeni mogu se posmatrati kao slični vaučerima: token se može zamijeniti za uslugu ili dobro koje pruža izdavalac^[8]. Prema tome, ova vrsta digitalnih tokena nema ulogu sredstva plaćanja ili razmjene na digitalnom tržištu, iz čega dalje proizilazi da njihova vrijednost ne zavisi od volatilnosti tržišta digitalne imovine već od funkcionalne vrijednosti usluge ili dobra kom omogućava pristup.

Sigurnosni tokeni su „imovina, kao što je potraživanje po osnovu duga ili vlasničkog udjela kod izdavaoca. Po svojoj ekonomskoj funkciji, ovi tokeni su analogni akcijama, obveznicama ili derivativnim finansijskim instrumentima”^[9]. Tipično, emitovanje sigurnosnih tokena posredstvom *blockchain* tehnologije predstavlja

način za privredna društva da prikupe kapital. Na primjer, tZERO token je sigurnosni token koji svom vlasniku daje vlasnička prava u *tZERO Group Inc*^[10].

Na kraju, s obzirom na značajan prostor koji otvaraju u pogledu zloupotrebe u svrhu prodaje falsifikovane imovine u elektronskoj trgovini, važno je još pomenuti imovinske (eng. *asset-backed tokens*) i nezamjenjive tokene (eng. *non-fungible tokens* – *NFTs*). Imovinski tokeni nastaju kao rezultat tokenizacije fizičke imovine u stvarnom svijetu (npr. nekretnina, nafte, zlata, dijamanta itd) i predstavljaju dokaz o vlasništvu ili udjelu u vlasništvu nad njom. Budući da svaki ovakav token predstavlja jednak udio u stvarnoj imovini koja je predmet tokenizacije (npr. proporcionalni dio u odnosu na ukupnu količinu zlata po osnovu koje su tokeni emitovani, izraženu u gramima), tj. ima istu ekonomsku vrijednost, on ima karakter zamjenjivosti, pa se može slobodno razmjenjivati za tokene iste klase^[11].

Nasuprot navedenom, “digitalna imovina koja je jedinstvena, a ne zamjenjiva, i koja se u praksi koristi kao kolekcionarski predmet, a ne kao sredstvo plaćanja ili investicioni instrument, može se označiti kao nezamjenjivi token (NFT) ili kriptokolekcionarski predmet”^[12]. Ovi tokeni predstavljaju strukturisane metapodatke koji se odnose na fizičke ili digitalne objekte, djeluju kao posebni identifikatori i često nisu neposredno povezani sa tim objektima.^[13] Primjera radi, nezamjenjivi tokeni se koriste za tržišno plasiranje digitalne umjetnosti – “oni sami po sebi nisu umjetnička djela, već sadrže hipervezu ka digitalnom ili fizičkom umjetničkom djelu, ali to ne podrazumijeva da je vlasnik tokena ujedno i vlasnik tog umjetničkog djela. Jedina stvar koju kupac stiče jeste sam token, dok se umjetničko djelo može pronaći samo putem veze sadržane u tokenu”^[14].

Iako savremene klasifikacije prepoznaju i druge vrste tokena, posebno mjesto u okviru digitalne ekonomije zauzimaju platni, uslužni i sigurnosni tokeni. Međutim,

sa stanovišta zloupotrebe digitalne imovine u prodaji falsifikovane robe u elektronskoj trgovini, najznačajniji su imovinski i nezamjenjivi tokeni. Ovi oblici digitalne imovine najčešće se koriste za prikrivanje porijekla i stvarne prirode robe, stvaranje privida autentičnosti ili plasiranje falsifikata pod oznakom „digitalno verifikovanih“ proizvoda.

[1] Član 2 stav 1 tačka 2 Zakona.

[2] Član 2 stav 1 tačka 3 Zakona.

[3] Stoyka, M. (2021). Cryptocurrency – definition, functions, advantages and risks. *Pidpriemnytstvo i Torhivlia*, 30, 5–10. Dostupno na: <https://doi.org/10.36477/2522-1256-2021-30-0>.

[4] Garrido, J. M. (2023). *Digital Tokens: A Legal Perspective* (IMF Working Paper No. WP/23/151). Međunarodni monetarni fond. Dostupno na: <https://www.imf.org/en/Publications/WP/Issues/2023/03/10/Digital-Tokens-A-Legal-Perspective-530220>.

[5] Ibidem.

[6] Izzah, W. N., Fokri, W. M., Muhammad, E., Ali, T. E., Nordin, N., Yusof, W. M., Chik, W., Aziz, S. A., Jazlan, A., i Jusoh, M. (2021.) Classification of cryptocurrency: A review of the literature. *Turkish Journal of Computer and Mathematics Education*, 12(5), 1183–1190. Dostupno na: <https://www.mendeley.com/catalogue/8599b843-d7f6-3d36-8cbf-b1e44a30089b/>.

[7] Član 3 stav 1 tačka 8 MiCA. Dostupna na: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/hrv>. MiCA je prvi sveobuhvatni pravni akt EU koji definiše pojam kriptoimovine. Stupila je na snagu 29. juna 2023. godine, a njene odredbe se u potpunosti primjenjuju od 30. decembra 2024. godine.

[8] Garrido, J. M. (2023). *Digital Tokens: A Legal Perspective* (IMF Working Paper No. WP/23/151). Međunarodni monetarni fond.

[9] van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, 9(22). Dostupno na: <https://doi.org/10.1186/s40854-022-00432-8>.

[10] Vidi na: <https://tzero.com/>.

[11] Naravno, zamjenjivi tokeni mogu se zamijeniti i za stvarnu imovinu koju predstavljaju (u konkretnom slučaju zlato).

[12] Financial Action Task Force (FATF). (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. Pariz: FATF. Dostupno na: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html>.

[13] Vidi: Idelberger, F. i Mezei, P. (2022). Non-fungible tokens. *Internet Policy Review*, 11(2). Dostupno na: <https://doi.org/10.14763/2022.2.1660>.

[14] Garrido, J. M. (2023). *Digital Tokens: A Legal Perspective* (IMF Working Paper No. WP/23/151). Međunarodni monetarni fond.

2. MEHANIZMI ZLOUPOTREBE DIGITALNE IMOVINE U PRODAJI FALSIFIKOVANE ROBE

Razvoj interneta i na njemu zasnovanih tehnologija omogućio je zamajac digitalne ekonomije i pojavu novih i inovativnih modela poslovanja.^[1] Međutim, brza ekspanzija elektronske trgovine, podstaknuta imperativom globalizacije tržišta, donijela je istovremeno nove mogućnosti i izazove. Među izazovima se ističe rasprostranjena i olakšana prodaja falsifikovane robe, zahvaljujući jedinstvenim karakteristikama digitalnih platformi, poput anonimnosti, prekogranične dostupnosti i brzine transakcija. U tom kontekstu, povrede prava intelektualne svojine imaju ključnu ulogu jer upravo one omogućavaju da se falsifikovana roba plasira kao autentična, na koji način se potrošači dovode u zabludu.

U cilju lakšeg prometa falsifikovane robe u okvirima elektronske trgovine, među pravima intelektualne svojine najčešće se zloupotrebljava pravo žiga, tj. pravo kojim se štiti znak koji u prometu služi za razlikovanje roba, odnosno usluga jednog pravnog ili fizičkog lica od iste ili slične robe, odnosno usluga drugog pravnog ili fizičkog lica^[2]. Žig se može sastojati od riječi, ličnih imena, slogana, slova, brojeva, slika, crteža, boje, rasporeda boja itd. Razlog zbog kog se upravo žig najčešće zloupotrebljava leži u njegovoj funkciji garancije prepoznatljivosti i povjerenja potrošača, naročito u uslovima elektronske trgovine, koji podrazumijevaju da kupac nije u mogućnosti da vidi proizvod. Iza upotrebe žiga se, dakle, nalaze i odnos povjerenja i pretpostavka kvaliteta, koji su od strane nosioca žiga pažljivo građeni usvajanjem određenih koncepata i standarda poslovanja i plasiranja proizvoda i usluga, kao i tradicije kvaliteta.^[3]

Pored povreda prava intelektualne svojine, promet falsifikovane robe u elektronskoj trgovini dodatno je olakšan razvojem i upotrebom digitalne imovine, naročito kriptovaluta, koja nije samo sredstvo plaćanja već i instrument prikrivanja stvarne prirode trgovinskih aktivnosti, što u značajnoj mjeri doprinosi opstanku i širenju tržišta falsifikovane robe.

[1] Čeranić Perišić, J. (2020). *Izazovi prodaje robe na platformama za elektronsku trgovinu – s posebnim osvrtom na prodaju krivotvorene robe putem interneta*. U: D. D. Vukadinović (ur.), *Liber amicorum in honour of Radovan D. Vukadinović: Izazovi u međunarodnom poslovnopravnom pravu i pravu Evropske unije* (str. 77–92). Akademija nauka i umjetnosti Republike Srpske i Udruženje za evropsko pravo. Dostupno na: <http://ricl.iup.rs/300/>.

[2] Član 2 stav 1 Zakona o žigu ("Službeni list Crne Gore", br. 072/10 od 08.12.2010, 044/12 od 09.08.2012, 018/14 od 11.04.2014, 040/16 od 30.06.2016, 002/17 od 10.01.2017, 003/23 od 10.01.2023, 084/24 od 06.09.2024).

[3] Reljanović, M. (2024). Odgovornost hosting provajdera za povredu žiga – pravni okvir i praksa u Republici Srbiji. *Intellectual Property and the Internet 2017*. Dostupno na: <http://ricl.iup.rs/980/3/2016%20-%20Internet%20-%20Reljenovi%C4%87.pdf>.

2.1. OSOBINE DIGITALNE IMOVINE KOJE POGODUJU ZLOUPOTREBI

Nekoliko je ključnih karakteristika digitalne imovine zbog kojih se često ispostavlja kao saveznik u prometu falsifikovane robe u elektronskoj trgovini. Najvažnija, naročito na terenu digitalne imovine zasnovane na *blockchain* tehnologiji, jeste pseudoanonimnost učesnika u transakcijama – njihov identitet ostaje skriven iza alfanumeričkih oznaka, što značajno otežava mogućnost identifikacije stvarnih korisnika i praćenja porijekla sredstava. Primjera radi, kada korisnik A pošalje korisniku B iznos od 10.000 USDT na *Ethereum* mreži, *blockchain* javno bilježi da je izvršena transakcija između adrese pošiljaoca „ox4fA3...B29e“ i adrese primaoca „ox9cD8...7F21“, pri čemu čuva podatke o tačnom iznosu te transakcije, vremenu njenog izvršenja, te visini naknade za njenu obradu koja pripada *Ethereum* mreži (tzv. naknada za gas, eng. *gas fee*). Dakle, *blockchain* ne evidentira nijedan podatak na osnovu koga bi se mogao otkriti identitet lica A i lica B.

Naravno, ovo se ne odnosi na slučajeve kada se digitalna imovina razmjenjuje putem centralizovanih kriptomjenjačnica koje sprovode postupak identifikacije korisnika – KYC (npr. *Binance*, *Coinbase* itd), što omogućava da se naknadno poveže određena adresa sa stvarnim identitetom njenog vlasnika. Takođe, postoje određene metode koje tajne službe i vladine agencije koriste kako bi utvrdile ko je koristio određenu adresu digitalnog novčanika (eng. *wallet address*)^[1], pa možemo reći da princip pseudoanonimnosti nije do kraja sproveden^[2]. Ipak, realizovan je u mjeri dovoljnoj da omogućava visok stepen prikrivanja identiteta kupca i prodavca na digitalnom tržištu zbog čega predstavlja jedan od ključnih faktora koji olakšavaju promet falsifikovane robe u elektronskoj trgovini.

Još jedna od specifičnosti digitalne imovine jeste mogućnost njene razmjene putem *peer-to-peer* (P2P) sistema i decentralizovanih berzi (DEX). P2P označava model direktne komunikacije i razmjene između korisnika, bez posredovanja centralnog subjekta, kao što su banke ili druge finansijske institucije, koje bi mogle da nadgledaju, verifikuju ili blokiraju transakcije. Dakle, korisnici međusobno obavljaju transakcije koristeći softversku infrastrukturu koja povezuje njihove digitalne novčanike, dok se podaci o transakcijama bilježe u decentralizovanoj mreži.

Sa druge strane, DEX predstavljaju razvijeniji oblik P2P sistema, koji omogućava trgovinu različitim vrstama kriptovaluta i tokena posredstvom pametnih ugovora (eng. *smart contracts*) – automatizovanih programskih kodova koji izvršavaju transakcije kada su ispunjeni unaprijed definisani uslovi^[3].

Na zloupotrebe povezane sa virtuelnom imovinom utiče i činjenica da su učesnici na tržištu često lica iz različitih država u kojima ne postoje efikasni mehanizmi kontrole pranja novca i koje karakteriše odsustvo centralnog posrednika, odnosno izdavaoca.^[4] U skladu sa tim, za razliku od tradicionalnog sistema finansija, kriptovalute karakteriše decentralizovanost, što značajno otežava praćenje porijekla sredstava i sprečavanje nezakonitih aktivnosti a čini ih pogodnim za upotrebu u svrhu prometa falsifikovane robe u digitalnom tržišnom prostoru.

Nadalje, globalni domet i brzina transakcija u okviru kojih se digitalna imovina, prema volji učesnika transakcija, koristi kao sredstvo plaćanja naročito doprinose njenoj zloupotrebi radi prodaje falsifikovane robe na internetu. Dok su tradicionalne bankarske transakcije, naročito međunarodne, predmet obrade nekoliko sati ili dana, savremene *blockchain* mreže, poput *Ripple* ili *Stellar*, omogućavaju potvrdu transakcije u svega nekoliko sekundi, uz mogućnost obrade više od hiljadu transakcija u jednoj sekundi^[5]. Posljedično, prodavcima falsifikovane robe omogućeno je da posluju sa kupcima širom svijeta, uz izbjegavanje tradicionalnih finansijskih mehanizama kontrole što doprinosi ekspanziji elektronskog tržišta falsifikovane robe.

Naredna karakteristika digitalne imovine koja pogoduje njenoj zloupotrebi u svrhu prodaje falsifikovane robe na digitalnom tržištu jeste nepovratnost transakcija. Za razliku od tradicionalnih platnih sistema koji omogućavaju korisniku povraćaj sredstava u slučaju prevare ili greške, jednom kada se transakcija digitalnom imovinom potvrdi i kada je *blockchain* memoriše, ona se ne može izmijeniti, poništiti ili opozvati. Ovakva nepovratnost transakcija zasniva se na tehničkoj strukturi *blockchain* sistema, koji primjenjuje koncept trostrukog knjigovodstva radi trajnog pohranjivanja transakcija, pri čemu se njihova autentičnost i nepromjenjivost obezbjeđuju korišćenjem kriptografije javnog ključa^[6].

Upravo zbog toga, prodavci koji su kupcima predali falsifikovanu robu, a zauzvrat stekli kontrolu nad digitalnom imovinom, istovremeno stižu i potpunu sigurnost da će takvu kontrolu i zadržati, dok kupci ostaju bez pravnog i tehničkog mehanizma za povraćaj novca nakon što uoče da su kupili neautentičan proizvod. Odsustvo mogućnosti povraćaja sredstava i institucionalne zaštite kupca smanjuje rizik za prodavce falsifikata i povećava isplativost njihovog poslovanja u digitalnom okruženju. Na taj način, nepovratnost transakcija ne samo da otežava otkrivanje i sankcionisanje prevara, već i podstiče porast obima trgovine falsifikovanim robom, jer pruža dodatni nivo sigurnosti onima koji se bave njenom prodajom na internetu.

Na kraju, za potrebe ovog rada istaći ćemo još jedno. U savremenoj finansijskoj industriji razvija se novi koncept – tokenizacija različitih oblika imovine, kojom se razmjena imovine sprovodi posredstvom javne *blockchain* infrastrukture^[7], a koja značajno doprinosi složenosti fenomena zloupotrebe digitalne imovine u elektronskoj trgovini. Pojam „tokenizacija“ odnosi se na proces povezivanja referentne imovine sa kriptotokenima putem mehanizama dizajna koji vezuju cijenu tokena za vrijednost imovine na koju se odnosi^[8]. Drugim riječima, tokenizacija je proces u kojem se određeni predmet, pravo ili vrijednost iz stvarnog svijeta digitalno „pretvara“ u token na *blockchain* mreži i to najčešće u obliku ranije pomenutog nezamjenjivog tokena ili imovinskog tokena. Svaki token sadrži niz podataka koji ga povezuju sa predmetom tokenizacije (serijski broj, slika, opis itd), a svaki nosilac kriptotokena ima pravno obavezujuće vlasničko pravo nad imovinom na koju se token odnosi^[9]. Takva tehnološka mogućnost podrazumijeva, između ostalog, stvaranje tržišta digitalne umjetnosti, luksuznih predmeta i sl, koji se mogu kupovati i prodavati globalno, bez njihovog fizičkog prisustva.

Međutim, upravo ta osobina stvara prostor za zloupotrebu tokenizacije kao sredstva stvaranja privida autentičnosti. Naime, u praksi ne postoji tehnički mehanizam koji bi osigurao da predmet koji je tokenizovan zaista postoji, niti da je autentičan - *blockchain* samo potvrđuje postojanje digitalnog zapisa, ali ne i autentičnost informacija koje su u njega unešene, na koji način se otvara mogućnost da prodavci falsifikovane robe tokenizuju neautentične proizvode i plasiraju ih na tržište kao tzv. digitalno verifikovane.

Na primjer, prodavac može tokenizovati falsifikat luksuznog sata i izdati nezamjenjivi token koji sadrži njegovu fotografiju i QR kod koji vodi ka digitalnom zapisu o tokenu pohranjenom na *blockchain* mreži. Na prvi pogled, kupac vidi oznaku „verifikovano putem *blockchain* tehnologije“ (eng. *blockchain verified*) i vjeruje da je riječ o originalnom proizvodu, iako takav token potvrđuje samo činjenicu da je digitalni zapis izdat a ne da sat zaista potiče od proizvođača čiji žig nosi. Ovakve prakse otvaraju niz pravnih pitanja u pogledu povrede prava intelektualne svojine, naročito prava žiga, jer lica bez odobrenja nosilaca prava mogu jednostavno reprodukovati ili nuditi na prodaju nezamjenjive tokene koji vizuelno oponašaju proizvode poznatih brendova. Takvi neovlašćeno kreirani digitalni zapisi, koji sadrže zaštićene žigove, logotipe ili dizajnerska rješenja, stvaraju lažan utisak autentičnosti i predstavljaju ozbiljan rizik za nosioce prava, budući da mogu dovesti do zavaravanja potrošača i narušavanja reputacije brenda. [\[10\]](#)

Zloupotrebe ove vrste naročito su olakšane zbog nedostatka jasnog regulatornog okvira i nadzora nad tržištem tokenizovane imovine. U većini jurisdikcija još uvijek ne postoji pravno obavezujuća definicija zamjenjivog tokena, niti se precizno uređuje njihova pravna priroda, obaveze izdavaoca ili odgovornost platformi koje njima trguju. Isto važi i za imovinske tokene, kod kojih pravni status osnovne imovine često ostaje neprovjerljiv, što omogućava da se trgovina tokenizovanom imovinom odvija bez stvarne kontrole i predstavlja plodno tlo za plasman falsifikovane robe i pranje novca kroz digitalne kanale. U tom smislu, tokenizacija imovine, iako tehnološki inovativna i potencijalno korisna za razvoj tržišta kapitala u nedostatku regulacije postaje jedan od najefikasnijih mehanizama za prikrivanje nezakonite trgovine u digitalnom prostoru.

Dakle, može se uočiti da zloupotrebe digitalne imovine u prodaji falsifikovane robe proizilaze iz njenih suštinskih tehničkih karakteristika – prije svega pseudoanonimnosti, decentralizovanosti, globalne dostupnosti, nepovratnosti transakcija i mogućnosti tokenizacije imovine bez prethodne provjere autentičnosti. Te osobine, iako u osnovi unapređuju brzinu, efikasnost i dostupnost digitalnih tržišta, istovremeno stvaraju prostor za pravnu nesigurnost i omogućavaju različite oblike zloupotreba u sferi elektronske trgovine.

S obzirom na to da postojeći pravni i institucionalni okviri nijesu u dovoljnoj mjeri prilagođeni dinamičnom razvoju digitalne ekonomije, neophodno je pristupiti izradi preciznijih normativnih rješenja i mehanizama nadzora koji bi ograničili mogućnost takvih zloupotreba a istovremeno očuvali inovativni potencijal *blockchain* tehnologije.

[1] Dodatno, Radna grupa za finansijsku akciju (FATF) je uvela tzv. *Travel Rule* - obavezu pružalaca usluga povezanih sa virtuelnom imovinom (eng. *Virtual Asset Service Providers – VASPs*) da prilikom izvršenja ili prijema transfera digitalne imovine prikupe i razmjenjuju osnovne podatke o pošiljaocu i primaocu transakcije (obično ime, adresu i broj računa pošiljaoca, kao i ime i broj računa primaoca), kao i da omoguće da te informacije, ukoliko je potrebno, budu dostupne nadležnim organima, naročito onim u čijoj je nadležnosti sprovođenje mjera protiv pranja novca i finansiranja terorizma. Ova mjera ima za cilj da omogući pravovremeno otkrivanje i praćenje sumnjivih tokova sredstava, uključujući one koji potiču iz nezakonitih aktivnosti poput prodaje falsifikovane robe u okviru elektronske trgovine. Nažalost, primjena ovog pravila u praksi i dalje je vrlo ograničena, naročito imajući u vidu činjenicu da se značajan dio transakcija odvija posredstvom decentralizovanih mreža koje nisu obuhvaćene ovim režimom. Vidi: Financial Action Task Force (FATF). (2025). *Best Practices on Travel Rule Supervision*. Pariz: FATF. Dostupno na: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf>.

[2] Cunjak Mataković, I. i Mataković, H. (2018). Kriptovalute - sofisticirani kodovi manipulacije. *International Journal of Digital Technology & Economy*, 3(1), 23-37. Dostupno na: <https://hrcak.srce.hr/216173>.

[3] Njihov je glavni cilj je da ugovorni odnos učine efikasnijim i ekonomski isplativijim, sa manje mogućnosti za greške, odlaganja ili sporove. Vidi: Cvetković, P. (2020). Pravni aspekti primene blokčejna: primer pametnih ugovora. *Pravna riječ*, XVII (63). Banja Luka: Udruženje pravnika Republike Srpske. Dostupno na: https://up-rs.org/wp-content/uploads/2024/01/PRAVNA_RIJEC_63_20.pdf.

[4] Kostic, Jelena. (2023). Misuse of Digital Assets: Current Legislation, Challenges and Recommendations. *Regional Law Review*, 2023, 375-388. Dostupno na: <http://ricl.iup.rs/1802/>.

[5] Hazari, S. S. i Mahmoud, Q. H. (2020). Improving transaction speed and scalability of blockchain systems via parallel proof of

work. *Future Internet*, 12(8), 125. Dostupno na: <https://doi.org/10.3390/fi12080125>.

[6] Gamage, H. T. M., Weerasinghe, H. D. i Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. *SN Computer Science*, 1(114). Dostupno na: <https://doi.org/10.1007/s42979-020-00123-0>.

[7] Ross, O., Jensen, J. R. i Asheim, T. (2019). *Assets under tokenization: Can blockchain technology improve post-trade processing?* University of Copenhagen i eToroX Labs. SSRN. Dostupno na: <https://ssrn.com/abstract=3488344>.

[8] Carapella, F., Chuan, G., Gerszten, J., Hunter, C. i Swem, N. (2023). *Tokenization: Overview and financial stability implications*. Finance and Economics Discussion Series 2023-060. Vašington: Board of Governors of the Federal Reserve System. Dostupno na: <https://doi.org/10.17016/FEDS.2023.060>.

[9] Ibid.

[10] Vidi: Kim, S. (2023). Counterfeit NFTs and brand protection. *Journal of Virtual IP Law*, 18(1), 72.

3. PREPORUKE ZA UNAPRJEĐENJE REGULATORNOG I NADZORNOG OKVIRA

Uzimajući u obzir kompleksnost zloupotreba digitalne imovine u okviru elektronske trgovine, posebno u pogledu prodaje falsifikovane robe i prikrivanja njenog porijekla, jasno je da postojeći regulatorni i nadzorni mehanizmi nijesu prilagođeni dinamičnom razvoju tržišta digitalnih sredstava. Pravni sistemi u regionu i šire još uvijek u velikoj mjeri tretiraju digitalnu imovinu kroz prizmu tradicionalnih finansijskih instrumenata, dok pojedini pravni poreci digitalnu imovinu ne prepoznaju uopšte, ili je prepoznaju fragmentarno, bez jasnog definisanja njene pravne prirode i nadzornog režima. Stoga je neophodno pristupiti sveobuhvatnom unapređenju regulatornog i nadzornog okvira što bi istovremeno omogućilo prevenciju zloupotreba i očuvanje inovativnog potencijala *blockchain* tehnologije.

Prvo, neophodno je normativno uspostaviti definiciju instituta tokenizovane imovine i uvesti obavezu verifikacije stvarne imovine na koju se token odnosi (tzv. referentne imovine) a sve u cilju sprječavanja prakse kreiranja prividno verifikovane robe putem tokenizacije. Donošenjem posebnih podzakonskih akata trebalo bi propisati obavezu izdavalaca tokena da dostave dokaze o postojanju i autentičnosti referentne imovine, kao i da budu registrovani kod nadležnog organa. Takav sistem verifikacije spriječio bi zloupotrebe u kojima se tokeni izdaju za nepostojeću ili falsifikovanu robu, čime bi se smanjio rizik od obmane potrošača.

Drugo, efikasna primjena mjera protiv pranja novca zahtijeva da se tzv. *Travel Rule*, kao međunarodni standard, primijeni i na decentralizovane berze i *peer-to-peer* mreže koje omogućavaju prenos digitalne imovine. Time bi se obezbijedilo da osnovni podaci o pošiljaocu i primaocu transakcije budu dostupni i u sistemima koji funkcionišu bez centralnog posrednika, što bi značajno unaprijedilo mogućnost praćenja tokova sredstava i otkrivanja sumnjivih aktivnosti. S tim u vezi, potrebno je razviti tehničke standarde interoperabilnosti između pružalaca usluga povezanih sa virtuelnom imovinom (VASPs) i decentralizovanih mreža.

Treće, radi jačanja transparentnosti tržišta i nadzorne funkcije države, preporučuje se formiranje nacionalnog registra digitalne imovine, koji bi obuhvatio sve licencirane pružaoce usluga. Takav registar omogućio bi korisnicima da provjere pouzdanost subjekata sa kojima posluju, a nadležnim organima lakši pristup podacima o prometu digitalne imovine. Poseban dio registra mogao bi se odnositi na tržište tokenizovane imovine, uz obavezu javne objave osnovnih podataka o predmetu tokenizacije i njegovoj verifikaciji.

I četvrto, da bi se na efikasan način suzbile nezakonite aktivnosti povezane sa digitalnom imovinom, neophodno je intenzivno raditi na izgradnji institucionalnih kapaciteta, tj. osnovati specijalizovane jedinice za digitalni nadzor unutar organa finansijskog nadzora, uprava za sprečavanje pranja novca i policijskih struktura koje bi raspolagale ekspertizom u oblasti *blockchain* analitike i kriptoforenzike. Istovremeno, preporuka je da se uspostave mehanizmi međuinstitucionalne saradnje između regulatora, poreskih uprava i organa za zaštitu intelektualne svojine, kako bi se obezbijedio integrisan pristup praćenju i sankcionisanju zloupotreba.

Na kraju, jasno je da se uspješno suprotstavljanje zloupotrebama digitalne imovine ne može postići izolovanim pristupima, već zahtijeva kombinaciju regulatornih, tehničkih i institucionalnih mjera. Ipak, neophodno je opredijeliti se za pažljivo izbalansiran pristup koji će, sa jedne strane, omogućiti efikasan nadzor i sprječavanje zloupotreba, a sa druge očuvati podsticajno okruženje za inovacije i dalji razvoj tržišta digitalne imovine.

Zloupotreba digitalne imovine u prodaji falsifikovane robe predstavlja složen i višedimenzionalan izazov savremenog digitalnog tržišta. Taj izazov proizilazi iz tehničkih osobina digitalne imovine koje omogućavaju visok stepen anonimnosti, brzine i globalnog dosega ali i iz nedovoljno razvijenog regulatornog okvira koji još uvijek pokušava da uhvati korak sa tehnološkim inovacijama.

Prodaja falsifikovane robe putem digitalnih kanala pokazuje da svaka tehnološka inovacija, pored koristi, otvara i nova polja rizika, čemu posebno doprinose različiti vidovi zloupotreba digitalne imovine. Ipak, uprkos pravnim i tehničkim izazovima koje donosi, digitalna imovina više nije prolazna pojava, već realnost globalne ekonomije. Njena uloga u razvoju novih tržišta, finansijskih instrumenata i oblika poslovanja je neosporna. Zbog toga rješenje ne može biti u njenom potiskivanju, već u razumijevanju, praćenju i postepenom oblikovanju pravnog i institucionalnog okvira koji će omogućiti njenu bezbjednu i odgovornu upotrebu.

Dakle, uspješno suprotstavljanje zloupotrebama digitalne imovine zahtijeva sveobuhvatan pristup. Samo balansiranom kombinacijom regulacije i slobode inovacija moguće je obezbijediti da digitalna imovina ne bude instrument obmane i nezakonitosti već pokretač daljeg razvoja digitalne ekonomije.

I NAUČNI ČLANCI

1. Bagić, K. (2018). Kriptogram – vrlo kratak uvod. *Croatica*, 42 (62), 343-364. <https://doi.org/10.17234/Croatica>.
2. Budimir, N. (2020). Blockchain tehnologija u osiguranju. *Elektronički zbornik radova Veleučilišta u Šibeniku*, 14 (1-2), 171-181. <https://hrcak.srce.hr/241621>.
3. Carapella, F., Chuan, G., Gerszten, J., Hunter, C. i Swem, N. (2023). *Tokenization: Overview and financial stability implications*. Finance and Economics Discussion Series 2023-060. Vašington: Board of Governors of the Federal Reserve System. <https://doi.org/10.17016/FEDS.2023.060>.
4. Cumming, D. J., Johan, S. i Pant, A. (2019). Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty. *Journal of Risk and Financial Management*, 12(3), 126. <https://doi.org/10.3390/jrfm12030126>.
5. Cunjak Mataković, I. i Mataković, H. (2018). Kriptovalute - sofisticirani kodovi manipulacije. *International Journal of Digital Technology & Economy*, 3(1), 23-37. <https://hrcak.srce.hr/216173>.
6. Cvetković, P. (2020). Pravni aspekti primene blokčejna: primer pametnih ugovora. *Pravna riječ*, XVII (63). Banja Luka: Udruženje pravnika Republike Srpske. https://up-rs.org/wp-content/uploads/2024/01/PRAVNA_RIJEC_63_20.pdf.
7. Ćeranić Perišić, J. (2020). Izazovi prodaje robe na platformama za elektronsku trgovinu – s posebnim osvrtom na prodaju krivotvorene robe putem interneta. U: D. D. Vukadinović (ur.), *Liber amicorum in honour of Radovan D. Vukadinović: Izazovi u međunarodnom poslovnopravnom pravu i pravu Evropske unije* (str. 77–92). Akademija nauka i umjetnosti Republike Srpske i Udruženje za evropsko pravo. <http://ricl.iup.rs/300/>.
8. Hazari, S. S. i Mahmoud, Q. H. (2020). Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Future Internet*, 12(8), 125. <https://doi.org/10.3390/fi12080125>.
9. Garrido, J. M. (2023). Digital Tokens: A Legal Perspective (IMF Working Paper No. WP/23/151). Međunarodni monetarni fond. <https://www.imf.org/en/Publications/WP/Issues/2023/03/10/Digital-Tokens-A-Legal-Perspective-530220>.
10. Hazari, S. S. i Mahmoud, Q. H. (2020). Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Future Internet*, 12(8), 125. <https://doi.org/10.3390/fi12080125>.
11. Idelberger, F. i Mezei, P. (2022). Non-fungible tokens. *Internet Policy Review*, 11(2). <https://doi.org/10.14763/2022.2.1660>.
12. Izzah, W. N., Fokri, W. M., Muhammad, E., Ali, T. E., Nordin, N., Yusof, W. M., Chik, W., Aziz, S. A., Jazlan, A., i Jusoh, M. (2021). Classification of cryptocurrency: A review of the literature. *Turkish Journal of Computer and Mathematics Education*, 12(5), 1183–1190. <https://www.mendeley.com/catalogue/8599b843-d7f6-3d36-8cbf-b1e44a30089b/>.
13. Kim, S. (2023). Counterfeit NFTs and brand protection. *Journal of Virtual IP Law*, 18(1), 72.

14. Kostic, Jelena. (2023). Misuse of Digital Assets: Current Legislation, Challenges and Recommendations. *Regional Law Review*, 2023, 375-388. <http://ricl.iup.rs/1802/>.
15. Jovanić, T. (2021). Kriptovalute kao novi izazov zaštite potrošača. *Zbornik radova Pravnog fakulteta Univerziteta u Beogradu*, str. 396–427. <https://plus.cobiss.net/cobiss/sr/sr/bib/39936009>.
16. Reljanović, M. (2024). Odgovornost hosting provajdera za povredu žiga – pravni okvir i praksa u Republici Srbiji. *Intellectual Property and the Internet 2017*. <http://ricl.iup.rs/980/3/2016%20-%20Internet%20-%20Reljenovi%C4%87.pdf>.
17. Ross, O., Jensen, J. R. i Asheim, T. (2019). Assets under tokenization: Can blockchain technology improve post-trade processing? University of Copenhagen i eToroX Labs. SSRN. <https://ssrn.com/abstract=3488344>.
18. Stoyka, M. (2021). Cryptocurrency – definition, functions, advantages and risks. *Pidpriemnytstvo i Torhivlia*, 30, 5–10. <https://doi.org/10.36477/2522-1256-2021-30-0>.
19. van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, 9(22). <https://doi.org/10.1186/s40854-022-00432-8>.
20. Zimonja, O. i Vujić, D. (2020). Kriptovalute – Izazovi aktuelnog globalnog trenda za kriminalističku praksu. *Kriminalistička teorija i praksa*, 7(2/2020), 55-71. <https://hrcak.srce.hr/252827>.

II NACIONALNI PROPISI

1. Zakona o digitalnoj imovini ("Službeni glasnik Republike Srbije", br. 153/2020). <https://www.paragraf.rs/propisi/zakon-o-digitalnoj-imovini.html>.
2. Zakon o žigu ("Službeni list Crne Gore", br. 072/10 od 08.12.2010, 044/12 od 09.08.2012, 018/14 od 11.04.2014, 040/16 od 30.06.2016, 002/17 od 10.01.2017, 003/23 od 10.01.2023, 084/24 od 06.09.2024). <https://www.gov.me/dokumenta/3876b715-b2ad-4ec3-9a62-a7983fbcce9f>.

III IZVORI MEĐUNARODNOG PRAVA

1. Direktiva (EU) 2018/843 Evropskog parlamenta i Savjeta od 30. maja 2018. godine o izmjeni Direktive (EU) 2015/849 o sprječavanju korišćenja finansijskog sistema u svrhu pranja novca i finansiranja terorizma, kao i o izmjeni direktiva 2009/138/EZ i 2013/36/EU. "Službeni list Evropske unije" L 156, 19.6.2018, str. 43–74. <https://eur-lex.europa.eu/eli/dir/2018/843/oj>.
2. Uredba (EU) 2023/1114 Evropskog parlamenta i Savjeta od 31. maja 2023. godine o tržištima kriptoimovine (*Markets in Crypto-assets – MiCA*). "Službeni list Evropske unije" L 150, 9.6.2023, str. 40–205. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>.

IV OSTALA LITERATURA

1. Financial Action Task Force (FATF). (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. Pariz: FATF. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html>.
2. Financial Action Task Force (FATF). (2025). *Best Practices on Travel Rule Supervision*. FATF, Pariz. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf>.