KRIPTOVALUTE KAO INFRASTRUKTURA ORGANIZOVANOG KRIMINALA

DOI: *10.70329/2744-2403.2026.6.11.14*

Izvorni naučni rad

Doc. dr. Zoran Kovačević [1]
Doc. dr. Zoran Lakić [2]

Sažetak:

Ovaj rad analizira transformativnu ulogu kriptovaluta u infrastrukturi savremenog organizovanog kriminala, argumentujući da blockchain tehnologija nije samo novi alat za stare kriminalne prakse, već da konstituiše kvalitativno novu kriminalnu ekonomsku arhitekturu koja mijenja temeljne odnose između kriminalnih aktera, žrtava i institucija. Kroz sistematsku analizu tehničkih mehanizama od Bitcoin pseudoanonimnosti i privacy coins, do DeFi protokola i cross-chain hopping tehnika, rad mapira evoluciju kriptovalutnog pranja novca od primitivnih jednokratnih transakcija prema sofisticiranim, višeslojnim operacijama koje kombinuju tehnološku sofisticiranost s institucionalnim ranjivostima globalnog regulatornog mozaika. Posebna analitička pažnja posvećena je slučajevima koji demonstriraju konvergenciju kriptokriminala s državnom strategijom, tj. ransomware koji funkcionišu kao paraziti na globalnoj digitalnoj ekonomiji, DeFi eksploatacijama koje u minutama dreniraju stotine miliona dolara, i sjevernokorejskim državno-sponzorisanim hakerskim operacijama koje finansiraju zabranjene oružane programe pod sankcijama. Rad evaluira regulatorne odgovore poput MiCA, FATF Travel Rule i OFAC sankcije, te identifikuje sistemske praznine koje ostavljaju DeFi i peer-to-peer sistem izvan efektivne regulatorne kontrole. Zaključak poziva na fundamentalnu promjenu paradigme regulatornog pristupa, i to od retrospektivne forenzike prema prospektivnoj arhitekturi transparentnosti koja mora biti ugrađena u same protokole.

Ključne riječi*: kriptovalute, blockchain forenzika, pranje novca, organizovani kriminal, privacy coins, DeFi, FATF, MiCA, ransomware, Lazarus Group.*

[1] Visoka poslovno tehnička škola Doboj, e-mail: zoran.kovacevic@dkpt.gov.ba
[2] Direkcija za koordinaciju policijskih tijela BiH, e-mail: zoran.lakic77@gmail.com

1. UVOD

Novac je uvijek bio centralni problem organizovanog kriminala, ne njegova zarada, već njegovo legitimiziranje. Istraživanje organizovanih kriminalnih grupa je oduvijek predstavljalo značajan izazov i problematiku za državne agencije i službe za provođenje zakona. Evolucija i prilagođavanje organizovanih kriminalnih grupa je uslovila i prilagođavanje agencija i službi koje se u značajnoj mjeri oslanjaju na obavještajni rad. Također, značaj i uloga modernih tehnologija, kao i društvenih mreža koje su neizostavni dio čovjekovog života, omogućavaju efikasnije prikupljanje operativnih podataka koji služe kao podrška istragama (Muhić, 2024). Od Al Kaponeovog pranja novca do suverenih offshore jurisdikcija 20. vijeka, čitava istorija finansijskog kriminala može biti čitana kao istorija potrage za mehanizmom koji će transformisati "prljavi" novac u "čisti". Pojava Bitcoina 2009. godine i naknadna eksplozija kriptovalutnog sistema nije bila s te perspektive, revolucija u punom smislu, jer su kriminalne organizacije i ranije koristile tehnološke inovacije za finansijske operacije. Ono što je, međutim, zaista revolucionarno jeste da kriptovalute ne samo da nude novi kanal za staru praksu pranja novca, već konstituišu novu ekonomsku arhitekturu koja fundamentalno mijenja ekonomiku kriminalnih finansija.

Tri strukturalna svojstva čine kriptovalute kvalitativno drugačijim instrumentom u fenomenologiji kriminalnih finansija od svih prethodnih platnih mehanizama. Prvo, decentralizacija eliminiše sam predmet klasičnih finansijskoobavještajnih intervencija, tj. ne postoji ni jedan entitet koji bi podlegao nalogu za zamrzavanje sredstava ili bio prisiljen otkriti identitet vlasnika adrese. Tamo gdje su tradicionalne metode suzbijanja pranja novca počivale na prinudnoj saradnji finansijskih posrednika, ovdje posrednika nema. Drugo, globalnost bez granica donosi drugu dimenziju operativne slobode, jer npr. transakcija između Pjongjanga i Brisela odvija se u minutama, jednakom brzinom i uz identične troškove kao lokalni transfer, bez ijednog regulisanog čvora kroz koji bi tok novca mogao biti presretnut. Treća karakteristika podrazumjeva fleksibilnost, te predstavlja onu distinkciju koja kriptovalute odvaja od svih analognih prethodnika na fundamentalan način. Kroz pametne ugovore i DeFi protokole, kriminalni akteri mogu konstruisati potpuno automatizovane operacije pranja novca koje se odvijaju bez ijednog ljudskog posrednika koji bi mogao biti regrutovan kao informator, stavljen pod pritisak ili procesno kompromitovan. Intuitivna kriminalistika omogućava istražiteljima da razmišljaju izvan ustaljenih okvira, što je posebno važno u rješavanju složenih slučajeva. Kreativni pristupi mogu otkriti nove metode i tehnike koje tradicionalni pristupi ne uzimaju u obzir (Korajlić, Selimić, Trnčić, Sahadžić, 2023). Akademska literatura o kriptovalutama i kriminalu rasla je eksponencijalno, od pionirskih radova (Möser, Böhme i Breuker, 2013)-(Spagnuolo, Maggi i Zanero, 2014), koji su uspostavili metodološke temelje "blockchain" forenzike, do sofisticiranijih analiza (Foley, Karlsen i Putniņš, 2019) koje su procijenile da je 25% Bitcoin korisnika u ranom

periodu bilo involvirano u nezakonite aktivnosti, ili Chainalysis godišnjih izvještaja koji su postali referentni empirijski izvor za regulatorne i sigurnosne institucije. Ovaj rad nastoji integrisati ovu literaturu s najnovijim empirijskim nalazima i evaluirati adekvatnost regulatornih odgovora razvijenih u periodu 2022-2024.

2. TEHNIČKA ANATOMIJA KRIPTOVALUTNOG PRANJA NOVCA

Jedna od najraširenijih zabluda o Bitcoin-u je jednako prisutna u popularnom diskursu kao i u nekim zatvorenim grupama, da je on anoniman. Ova zabluda bila je fatalna za neke rane kriminalne korisnike Bitcoin-a, konkretno Ross Ulbricht osnivača Silk Road-a uhapšenog 2013. godine, a FBI je zaplijenio Bitcoin u vrijednosti tadašnjih 28,5 miliona dolara, dijelom kroz blockchain forenziku koja je pratila transakcije do identifikovanih adresa (Christin, 2013; FBI, 2013). Blockchain je javna knjiga svih transakcija, beskompromisno djeljenje informacija u strukturalnom smislu, čak i dok skriva identitete iza pseudonimnih adresa. Međutim, redukovati kriptovalutnu forenziku na ovu razmjerno jednostavnu situaciju bilo bi analitički neodgovorno. Od tada su kriminalni akteri razvili sofisticirane tehničke mjere zaštite od blockchain forenzike koje su izmijenile forenzički pejzaž do neprepoznatljivosti. Centralne tehnike uključuju sljedeće: *CoinJoin i mixing servise* koji objedinjuju transakcije od višestrukih korisnika i emituju ih u rekombiniranim iznosima na nove adrese, kidajući forenzički lanac, *peeling chains* koji fragmentiraju velike iznose u serije malih transakcija prema stotinama adresa, i *chain hopping* koji konvertuje sredstva između različitih blockchain mreža npr. Bitcoin → Ethereum → Monero → Tether, umnožavaajući forenzičku kompleksnost svakom konverzijom.

Monero (XMR) predstavlja paradigmatski primjer privatnog novca koji je dizajniran od temelja za maksimalnu privatnost transakcija. Za razliku od Bitcoin-a, gdje je transparentnost zadana opcija a privatnost izuzetak, Monero implementira privatnost kao obaveznu karakteristiku protokola kroz tri komplementarne kriptografske tehnike i to: *Ring Signatures* koje skrivaju identitet pošiljaoca miješanjem s transakcijama decoys-a, *Stealth Addresses* koji generišu jednokratne adrese za svaku uplatu onemogućavajući linkovanje transakcija prema istom primaocu, i *Confidential Transactions (RingCT)* koji skrivaju iznose transakcija. Rezultat je da nijedan vanjski analitičar-stručnjak, uključujući sofisticirane kompanije poput Chainalysis, koje su javno potvrdile da nemaju pouzdane alate za Monero forenziku (Chainalysis, 2020), ne može pratiti tok sredstava. Ova karakteristika čini Monero preferiranom valutom za dark web tržišta i ransomware operatere koji zahtijevaju isplatu u XMR-u upravo zbog forenzičke neprobojnosti. Europol (2023) dokumentuje sistematičan prelazak darknet tržišta s Bitcoin-a na Monero, identifikujući ga kao dominantni izbor kriminalnih aktera kojima je operativna sigurnost primarni prioritet. Američka IRS ponudila je 2020. godine nagradu od 625.000 dolara za razvoj alata za

Monero forenziku, što je samo po sebi indikativan pokazatelj stepena u kojemu XMR predstavlja institucionalnu slijepu tačku (IRS, 2020).

Decentralizovane finansije (DeFi), sistem finansijskih aplikacija izgrađenih na programabilnim blockchain mrežama poput Ethereuma predstavljaju možda najkompleksniji regulatorni izazov koji je nastao iz kriptovalutne industrije. DeFi protokoli poput Uniswap, Aave, Compound i Tornado Cash operišu kao autonomni programi koji se izvršavaju na blockchainu bez centralnog operatera koji bi mogao biti pravno odgovoran, prisiljen na *KYC compliance* ili podvrgnut sankcijama. Kada je američki OFAC sankcionisao Tornado Cash 2022. godine, načinivši istorijski presedan sankcionisanja softvera umjesto fizičkih ili pravnih lica, što je izazvalo pravne kontroverze i relativno ograničeni operativni efekt, jer protokol nastavlja funkcionisati opstajući na blockchainu, izvan domašaja fizičke zabrane (U.S. Treasury, 2022; Van Loon v. Department of the Treasury, 2024). *Chainalysis* 2024. godine, dokumentuje da je 2023. godina bila rekordna po obimu pranja novca kroz DeFi kanale, s posebno izraženim trendom chain hopping-a koji koristi DEX protokole za konverziju između različitih blockchain sistema na način koji umnožava forenzičku kompleksnost.

3. RANSOMWARE - KRIPTOVALUTE KAO POSLOVNI MODEL

Ransomware, zlonamjerni softver koji enkriptuje podatke žrtve i zahtijeva kriptovalutno plaćanje za ključ dekriptiranja nije nova kriminalna pojava, ali ga je kriptovalutna ekonomija transformisala iz relativno marginalne taktike u industrijsku kriminalnu granu s procijenjenim globalnim troškovima od 20 milijardi dolara u 2023. godini (Cybersecurity Ventures, 2024). Ova transformacija nije slučajna jer upravo su kriptovalute, posebno Bitcoin i Monero, bile faktor koji je ransomware-u omogućio sigurnu monetizaciju kriminalnih operacija bez prolaska kroz regulisane finansijske kanale. Savremeni ransomware operiše prema modelu Ransomware-a-Service (RaaS), u kojemu kreatori zlonamjernog softvera licenciraju svoje alate koji sprovode napade i dijele prihode. Grupe poput LockBit, ALPHV/BlackCat, Clop i Royal operišu kao sofisticirani poslovni entiteti s korisničkim portalom za žrtve, tehničkom podrškom za pregovore o otkupnini i sofisticiranom kriptovalutnom *laundering* infrastrukturom. FBI, CISA i Europol uklonili su LockBit infrastrukturu u koordinisanoj operaciji februara 2024. godine, zaplijenivši 34 servera i identifikujući vodeće operatere, s timda da su eksplicitno upozorili da RaaS sistem posjeduje kapacitet za brzo rekonstituisanje (FBI/NCA, 2024).

Napad ransomware grupe DarkSide na Colonial Pipeline u maju 2021. godine, koji je prouzrokovao privremenu obustavu dostave goriva na istok SAD-a i isplatu otkupnine od 4,4 miliona dolara u Bitcoin-u, bio je paradigmatski primjer koji je demonstrirao sposobnost ransomware sistema da naruši funkcionisanje kritične

infrastrukture i iznudi isplate čiji je volumen bez istorijskog presedana (DOJ, 2021). Jednako indikativan kao i sam napad bio je naknadni djelomični povrat sredstava, jer FBI je uspio trasirati i zaplijeniti Bitcoin u vrijednosti 2,3 miliona dolara, što je demonstriralo i mogućnosti i granice blockchain forenzike, budući da je ostatak ostao nezaplijenjen (DOJ, 2021).

4. LAZARUS GROUP

Ransomware sistem, koliko god bio sofisticiran kao kriminalna industrija, ostaje u domenu privatnog kriminalnog poduzetništva motivisan profitom, organizovan horizontalno kroz partnerske mreže, podložan klasičnim mehanizmima krivičnog gonjenja. Sjevernokorejska hakerska grupa Lazarus Group predstavlja kvalitativno drukčiji fenomen koji zahtijeva posebnu analitičku kategoriju, jer ovdje država nije regulatorni akter koji progoni finansijski kriminal, već je sama neposredni izvršilac kriptovalutnih pljački čiji prihodi finansiraju program oružja za masovno uništenje. Ova inverzija normativnih uloga, gdje država kao kriminalni akter koristi kriptovalute za zaobilaženje međunarodnih sankcija, predstavlja možda najozbiljniji izazov koji je kriptovalutni sistem dosad postavio pred međunarodnu bezbjednosnu arhitekturu.

Lazarus Group djeluje pod okriljem Generalnog biroa za izviđanje (RGB), sjevernokorejske obavještajne agencije, i identificirana je kao odgovorna za niz sajber operacija koje su po obimu zaplijenjenih sredstava daleko prevazišle kapacitete privatnih kriminalnih organizacija. Chainalysis (2024) procjenjuje da je Lazarus Group u periodu 2017-2023. godine ukrala kriptovalute u ukupnoj vrijednosti između 3 i 4 milijarde dolara, što je iznos koji po obimu odgovara godišnjem bruto domaćem proizvodu nekoliko manjih država i koji UN Vijeće sigurnosti direktno vezuje za finansiranje sjevernokorejskog balističkog i nuklearnog programa (UN Security Council, 2024). Ova cifra nije špekulacija, već rezultat višegodišnje blockchain forenzike koju su paralelno provodili Chainalysis, američki Federalni istražni biro (FBI), Agencija za sajber sigurnost i sigurnost infrastrukture (CISA) i timovi Savjeta sigurnosti UN-a.

Također, Lazarus Group razvila je operativnu metodologiju koja se distinktivno razlikuje od ransomware modela po jednom ključnom obilježju, a to je da grupa ne iznuđuje, ona krade direktno, kroz tehničke eksploatacije blockchain infrastrukture čija sofisticiranost odražava državne obavještajne kapacitete, a ne individualne hakerske vještine. Napad na Ronin Network, blockchain most koji je podržavao popularnu igru Axie Infinity, izveden je u martu 2022. godine, čime je rezultirao krađom kriptovaluta u vrijednosti 625 miliona dolara, što ga čini najvećom pojedinačnom kriptovalutnom krađom u istoriji (FBI, 2022; Chainalysis, 2022). Metodologija napada demonstrirala je nivo sofisticiranosti koja je alarmirala i najiskusnije blockchain sigurnosne analitičare, jer Lazarus

Group je kroz period od više od godinu dana strpljivo kompromitirala validatorske čvorove mreže, pet od devet potrebnih za odobravanje transakcija, da bi zatim u jednoj koordinisanoj akciji autorizovala lažne isplate koje su iscrpile rezerve mosta.Napad na Harmony Horizon Bridge u junu 2022. godine, kojim je izvučeno 100 miliona dolara, te napad na Atomic Wallet u junu 2023. godine, sa gubicima od oko 35 miliona dolara, pokazali su da Ronin nije izolovan incident već dio sistemske strategije ciljanja tzv. blockchain mostova, tj. infrastrukturnih tačaka koje povezuju različite blockchain mreže i koje upravo zbog složenosti višestruke validacije, predstavljaju arhitekturalno najranjivije segmente kriptovalutnog sistema (UN Security Council, 2024). Ova precizna identifikacija i konzistentno ciljanje strukturalnih ranjivosti, a ne oportunistično iskorišćavanje slučajnih propusta, obilježje je operativnog profila koji odražava institucionalni, a ne individualni obavještajni kapacitet.

Jednako indikativan kao i sam modus operandi krađe jeste laundering proces koji Lazarus Group primjenjuje na ukradena sredstva, proces koji u svojoj sofisticiranosti i brzini egzekucije prevazilazi kapacitete svih poznatih privatnih kriminalnih organizacija. FBI i Chainalysis dokumentuju višeslojnu laundering infrastrukturu koja kombiniuje Tornado Cash i srodne protokole za inicijalno kidanje forenzičkog lanca (korišćeni i nakon OFAC sankcionisanja 2022. godine, što samo po sebi ilustruje granice jurisdikcionalne primjene sankcija), kao i serije cross-chain swap operacija između Ethereuma, Bitcoina i Monera, koje umnožavaju forenzičku kompleksnost i iscrpljuju analitičke resurse istraživača, te konačnu realizaciju kroz OTC brokere koji operišu u jurisdikcijama s minimalnom AML regulacijom posebno u Jugoistočnoj Aziji (Chainalysis, 2024; UN Security Council, 2024). Brzina kojom se ovaj lanac aktivira u pojedinim slučajevima unutar sati od izvršene krađe, ukazuje na unaprijed pripremljenu infrastrukturu koja nije improvizovana reaktivno, već planirana prospektivno kao sastavni dio operativne arhitekture napada.

Sankcionisanje Tornado Cash od strane OFAC-a 2022. godine, motivisano dijelom upravo dokumentovanim Lazarus Group korišćenjem tog protokola, demonstriralo je i doseg i granice sankcijskog oruđa, tj. sankcije su pogodile i legitimne korisnike koji su koristili protokol iz legitimnih razloga privatnosti, dok je sjevernokorejska hakerska infrastruktura relativno brzo adaptirala alternativne laundering kanale. Ovo nije argument protiv sankcionisanja, već argument za sistemsku regulatornu arhitekturu koja ne može počivati isključivo na reaktivnim mjerama usmjerenim na pojedinačne infrastrukturne tačke.

Analitički značaj Lazarus Group operacija prevazilazi dimenziju finansijskog kriminala i ulazi u domenu međunarodne sigurnosti. Procjene UN Panela eksperata iz 2024. godine, direktno povezuju kriptovalutne prihode Lazarus Group s finansiranjem sjevernokorejskog programa balističkih projektila i nuklearnog oružja, programa koji je međunarodnim sankcijskim režimom trebao

biti lišen finansijskog goriva (UN Security Council, 2024). Kriptovalutni sistem u ovom kontekstu, nije samo infrastruktura finansijskog kriminala, on je kanal za sankcijsku eroziju koja ugrožava arhitekturu međunarodnog mira i sigurnosti. Ova dimenzija zahtijeva da se regulatorna rasprava o kriptovalutama izvede iz isključivo finansijskog i pravnog okvira i pozicionira kao pitanje od neposrednog interesa za mehanizme kolektivne sigurnosti, uključujući Savjet bezbjednosti UN-a, čiji su mehanizmi sankcionisanja dosad demonstrirali ograničenu efektivnost u uslovima kriptovalutne ekonomije.

5. IZMEĐU NORMATIVNE AMBICIJE I OPERATIVNIH OGRANIČENJA

Finansijska akcijska radna grupa-FATF, koja postavlja globalne standarde protiv pranja novca, usvojila je 2019. godine proširenje tzv. Travel Rule na kriptovalutne transakcije, zahtijevajući od Virtual Asset Service Providers (VASP) da prikupljaju i razmjenjuju identifikacijske informacije o pošiljaocima i primaocima za transakcije iznad 1.000 dolara/eura, analogno pravilima koja već decenijama važe za bankarski sektor (FATF, 2019). Ova norma bila je značajan korak prema regulatornoj normalizaciji kriptovaluta, ali njena implementacijska stvarnost dramatično je divergirala od normativnih aspiracija. Problem nije u samom pravilu već u arhitekturalnoj ranjivosti njegova dosega. FATF, 2023. godine procjenjuje da je globalna usklađenost s Travel Rule još uvijek daleko ispod potrebnog praga, posebno u jurisdikcijama s niskim AML kapacitetima.

Markets in Crypto-Assets Regulation (MiCA), koji je stupio na snagu u EU 2024. godine, predstavlja najsveobuhvatniji regulatorni okvir za kriptovalutna tržišta usvojen bilo gdje u svijetu i važan iskorak prema integraciji kripto sektora u mainstreamu finansijsku regulativu (European Parliament, 2023). MiCA reguliše izdavanje kriptovaluta, pružaoce usluga kripto imovine (CASP) i stablecoinove, uspostavljajući KYC zahtjeve, kapitalnu adekvatnost i mehanizme zaštite potrošača. Međutim, analitičarska zajednica konzistentna je u identificiranju centralnog MiCA ograničenja, jer Uredba reguliše centralizovane aktere, ali nema efektivnog dosega nad DeFi protokolima koji operišu bez identificiranog "pružaoca usluge". Europska komisija eksplicitno je prepoznala ovaj nedostatak u MiCA tekstu, najavivši reviziju koja bi trebala adresirati DeFi do 2026. godine, ali ta revizija dolazi u uvjetima u kojima DeFi sektor raste eksponencijalno i u kojima su kriminalni akteri, uključujući i državno-sponzorisane grupe poput Lazarus Group, već etablirali sofisticirane DeFi-bazirane laundering infrastrukture (European Commission, 2024).

6. ZAKLJUČAK

Analiza kriptovaluta kao infrastrukture organizovanog kriminala demonstrira da regulatorni izazov nije samo tehničko pitanje razvoja boljih forenzičkih alata, već arhitekturalno kroz pitanje fundamentalnog promišljanja na kojim principima treba biti izgrađena regulatorna infrastruktura kriptovalutnog sistema. Retrospektivna forenzika, tj. identifikovanje kriminalnih tokova nakon što se dogode, strukturalno je inferiorna u uslovima u kojima se brzina transakcija mjeri u minutama, u kojima je *cross-chain* hopping slobodan i u kojima *privacy coins* nudi matematičku garanciju forenzičke neprobojnosti. Slučaj Lazarus Group to ilustruje s posebnom oštrinom, tj. kada je kriminalni akter državni aparat koji raspolaže obavještajnim kapacitetima i unaprijed pripremljenom infrastrukturom za pranje novca, retrospektivna forenzika dolazi uvijek prekasno.

Rješenje koje se nameće kao perspektivno jeste obavezna transparentnost porijekla sredstava ugrađena direktno u protokolni sloj, po uzoru na C2PA standard koji digitalne medije oprema verifikovanim metapodacima o izvoru. Takav pristup međutim pretpostavlja korjenitu redefiniciju temeljnog napetog odnosa između privatnosti i transparentnosti unutar kriptovalutnog sistema. Ova rekonfiguracija nije kozmetička regulatorna intervencija. Ona zadire u samu arhitektonsku logiku sistema i zahtijeva da se dva načela, koja su do sada tretirana kao procesno nepomirljiva, iznova uravnoteže kroz osmišljenu normativnu i tehničku intervenciju. Ovo je politički i normativno izuzetno složeno pitanje, jer legitimni argumenti za privatnost finansijskih transakcija nisu bezosnovani. Međutim, u uslovima u kojima kriptovalute postaju infrastruktura za finansiranje nuklearnih programa, ransomware napade na bolnice i pranje narkotičkog kapitala, pitanje optimalnog balansa između privatnosti i transparentnosti mora biti postavljeno kao centralni predmet demokratske deliberacije, a ne prepušteno da ga "de facto" rješavaju kriminalni akteri koji eksploatišu regulatorne praznine.

LITERATURA

1. Chainalysis, 2020. The Monero Tracing Challenge: Internal Assessment. Chainalysis Inc, https://www.chainalysis.com/blog/all-about-monero/(1.4.2026.).
2. Chainalysis, 2020. The Ronin Network Hack. Chainalysis Blog, https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/(1.4.2026.)
3. Chainalysis, 2024. The 2024 Crypto Crime Report. Chainalysis Inc., New York, https://go.chainalysis.com/crypto-crime-2024.html, (2.4.2026.)
4. Christin, N., 2013. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In Proceedings of WWW 2013. ACM.
5. Cybersecurity Ventures, 2024. Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031. Cybersecurity Ventures Annual Report. https://www.google.com/search?q=5.%09Cybersecurity+Ventures%2C+2024.+Global+Ransomware+Damage+Costs+Predicted+to+Exceed+%24265+Billion+by+2031, (3.4.2026.).
6. European Commission, 2024. Digital Finance Package: Review of MiCA and DeFi Regulatory Framework. COM(2024) 192 final.
7. European Parliament, 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). Official Journal of the EU, L 150.
8. Europol, 2023. Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol Spotlight Report, Den Haag. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies, (5.4.2026.)
9. FATF, 2019. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF/OECD, Paris.
10. FATF, 2023. Targeted Update on Implementation of FATF Standards on Virtual Assets/VASPs. FATF/OECD, Paris.
11. FBI / National Crime Agency, 2024. Operation Cronos: Disruption of LockBit Ransomware Group — Joint Press Release. https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant, (5.4.2026.).
12. FBI, 2013. Silk Road Takedown: United States v. Ross Ulbricht. DOJ Press Release, https://en.wikipedia.org/wiki/Silk_Road_(marketplace), (5.4.2026.).

13. FBI, 2022. FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Heist. Press Release, https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft, (6.4.2026.).
14. Foley, S., Karlsen, J. R. & Putniņš, T. J., 2019. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? Review of Financial Studies, 32(5), 1798–1853, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645, (6.4.2026.).
15. IRS Criminal Investigation, 2020. IRS CI Seeks Contractors for Monero-Tracing Pilot. Solicitation Number: 2032H321R00001.
16. Intelligence from the Bitcoin Spagnuolo, M., Maggi, F. & Zanero, S., 2014. BitIodine: Extracting Network. In Financial Cryptography and Data Security, Springer. https://static.miki.it/pdf/BitIodine_presentation.pdf, (7.4.2026.).
17. Korajlić, N., Selimić, M., Trnčić, L., Sahadžić, N., 2023. „ Značaj intuitivno kreativne kriminalistike u rješavanju kompleksnih krivičnih djela“, Zaštita i sigurnost, godina 3., broj 2., www.zisjournal.com.
18. Möser, M., Soska, K., Heilman, E. & Lee, K., 2018. An Empirical Analysis of Traceability in the Monero Blockchain. In Proceedings of the Workshop on Bitcoin Research. https://www.researchgate.net/publication/324863990_An_Empirical_Analysis_of_Traceability_in_the_Monero_Blockchain, (7.4.2026.).
19. Muhić, E., 2024. „ Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa“ Zaštita i sigurnost, godina 4., broj 2., www.zisjournal.com.
20. U.S. Department of Justice, 2021. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide. DOJ Press Release, (7.4.2026.).
21. U.S. Department of the Treasury – OFAC., 2022. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Press Release, (7.4.2026.).
22. UN Security Council. (2024). Final Report of the Panel of Experts on North Korea, S/2024/215. United Nations, New York.
23. Van Loon v. Department of the Treasury, 2024., No. 23-50669 (5th Cir. 2024), https://law.justia.com/cases/federal/appellate-courts/ca5/23-50669/23-50669-2024-11-26.html, (8.4.2026.).

CRYPTOCURRENCIES AS INFRASTRUCTURE FOR ORGANISED CRIME

DOI: *10.70329/2744-2403.2026.6.11.14*

Original Scientific Paper

Assoc. Prof. Dr Zoran Kovačević *

Assoc. Prof. Dr Zoran Lakić **

Abstract:

This paper analyses the transformative role of cryptocurrencies in the infrastructure of contemporary organised crime, arguing that blockchain technology is not just a new tool for old criminal practices, but constitutes a qualitatively new criminal economic architecture that changes the fundamental relationships between criminal actors, victims and institutions. Through a systematic analysis of the technical mechanisms from Bitcoin's pseudo-anonymity and privacy coins, to DeFi protocols and cross-chain hopping techniques, the work maps the evolution of cryptocurrency money laundering from primitive one-off transactions towards sophisticated, multi-layered operations that combine technological sophistication with the institutional vulnerabilities of the global regulatory mosaic. Particular analytical attention is paid to cases demonstrating the convergence of crypto-crime with state strategy, i.e. ransomware operating as parasites on the global digital economy, DeFi exploits that drain hundreds of millions of dollars in minutes, and North Korean state-sponsored hacking operations that fund banned weapons programs under sanctions. The paper evaluates regulatory responses such as MiCA, the FATF Travel Rule and OFAC sanctions, and identifies systemic gaps that leave DeFi and peer-to-peer systems outside effective regulatory control. The conclusion calls for a fundamental paradigm shift in the regulatory approach, from retrospective forensics to a prospective transparency architecture that must be built into the protocols themselves.

Keywords*: cryptocurrencies, blockchain forensics, money laundering, organised crime, privacy coins, DeFi, FATF, MiCA, ransomware, Lazarus Group.*

*Doboj Higher Business and Technical School, e-mail: zoran.kovacevic@dkpt.gov.ba
**Directorate for Coordination of Police Bodies of BiH, e-mail: zoran.lakic77@gmail.com

1. INTRODUCTION

Money has always been a central issue for organised crime, not its earning, but its legitimisation. The study of organised criminal groups has always presented a significant challenge and problem for state agencies and law enforcement services. The evolution and adaptation of organised criminal groups has necessitated the adaptation of agencies and services that rely heavily on intelligence work. Furthermore, the significance and role of modern technologies, as well as social networks which are an integral part of human life, enable the more effective collection of operational data that supports investigations (Muhić, 2024). From Al Capone's money laundering to the sovereign offshore jurisdictions of the 20th century, the entire history of financial crime can be read as a history of the search for a mechanism to transform "dirty" money into "clean" money. The emergence of Bitcoin in 2009 and the subsequent explosion of the cryptocurrency system was not, from this perspective, a revolution in the full sense, as criminal organisations had previously used technological innovations for their financial operations. What is truly revolutionary, however, is that cryptocurrencies not only offer a new channel for the old practice of money laundering, but also constitute a new economic architecture that fundamentally changes the economics of criminal finance.

Three structural properties make cryptocurrencies a qualitatively different instrument in the phenomenology of criminal finance from all previous payment mechanisms. First, decentralisation eliminates the very subject of classical financial intelligence interventions, i.e. there is no single entity that could be subject to an order to freeze funds or be compelled to disclose the identity of the address owner. Where traditional anti-money laundering methods relied on the compelled cooperation of financial intermediaries, here there are none. Secondly, borderless globality brings a second dimension of operational freedom, as a transaction between Pyongyang and Brussels, for example, takes place in minutes, at the same speed and for the same cost as a local transfer, without a single regulated node through which the money flow could be intercepted. The third characteristic is flexibility, and it represents the distinction that separates cryptocurrencies from all their analogue predecessors in a fundamental way. Through smart contracts and DeFi protocols, criminal actors can construct fully automated money laundering operations that take place without a single human intermediary who could be recruited as an informant, put under pressure, or procedurally compromised. Intuitive criminology allows investigators to think outside the box, which is particularly important in solving complex cases. Creative approaches can uncover new methods and techniques that traditional approaches do not take into account (Korajlić, Selimić, Trnčić, Sahadžić, 2023). Academic literature on cryptocurrencies and crime has grown exponentially, from pioneering works (Möser, Böhme and Breuker, 2013)- (Spagnuolo, Maggi, and

Zanero, 2014), which established the methodological foundations of "blockchain" forensics, to more sophisticated analyses (Foley, Karlsen, and Putniņš, 2019) which estimated that 25% of early Bitcoin users were involved in illicit activities, or the Chainalysis annual reports that have become a reference empirical source for regulatory and security institutions. This paper seeks to integrate this literature with the latest empirical findings and evaluate the adequacy of the regulatory responses developed in the 2022-2024 period.

2. THE TECHNICAL ANATOMY OF CRYPTOCURRENCY MONEY LAUNDERING

One of the most widespread misconceptions about Bitcoin is equally present in popular discourse as it is in some closed groups: that it is anonymous. This misconception was fatal for some early criminal users of Bitcoin; specifically, Ross Ulbricht, the founder of Silk Road, was arrested in 2013, and the FBI seized Bitcoin worth $28 million at the time. 5 million dollars, in part through blockchain forensics that traced transactions to identified addresses (Christin, 2013; FBI, 2013). The blockchain is a public ledger of all transactions, an uncompromising sharing of information in a structural sense, even as it hides identities behind pseudonymous addresses. However, to reduce cryptocurrency forensics to this relatively simple situation would be analytically irresponsible. Since then, criminal actors have developed sophisticated technical countermeasures against blockchain forensics that have changed the forensic landscape beyond recognition. Central techniques include the following: CoinJoin and mixing services that pool transactions from multiple users and broadcast them in recombined amounts to new addresses, breaking the forensic chain; and peeling chains that fragment large amounts into series of small transactions to hundreds of addresses, and chain hopping that converts funds between different blockchain networks, e.g., Bitcoin → Ethereum → Monero → Tether, multiplying the forensic complexity with each conversion.

Monero (XMR) is a paradigmatic example of a privacy coin designed from the ground up for maximum transaction privacy. Unlike Bitcoin, where transparency is the default option and privacy an exception, Monero implements privacy as a mandatory protocol feature through three complementary cryptographic techniques, namely: Ring Signatures, which hide the sender's identity by mixing with decoy transactions; Stealth Addresses, which generate one-time addresses for each payment, preventing transactions to the same recipient from being linked; and Confidential Transactions (RingCT), which hide transaction amounts. The result is that no external expert analyst, including sophisticated companies like Chainalysis, which have publicly confirmed that they do not have reliable tools

for Monero forensics (Chainalysis, 2020), can track the flow of funds. This feature makes Monero the preferred currency for dark web marketplaces and ransomware operators who demand payment in XMR precisely for its forensic-proof nature. Europol (2023) documents a systematic shift of darknet marketplaces from Bitcoin to Monero, identifying it as the dominant choice for criminal actors whose primary priority is operational security. In 2020, the US IRS offered a $625,000 reward for the development of Monero forensics tools, which is in itself an indicative indicator of the extent to which XMR represents an institutional blind spot (IRS, 2020).

Decentralized finance (DeFi), a system of financial applications built on programmable blockchain networks like Ethereum, represents perhaps the most complex regulatory challenge to have emerged from the cryptocurrency industry. DeFi protocols like Uniswap, Aave, Compound, and Tornado Cash operate as autonomous programs that run on the blockchain without a central operator who could be held legally responsible, forced to comply with KYC, or subjected to sanctions. When the U.S. OFAC sanctioned Tornado Cash in 2022, making the historic precedent of sanctioning software instead of physical or legal entities, it sparked legal controversies and a relatively limited operational effect, as the protocol continues to function, surviving on the blockchain, beyond the reach of a physical ban (U.S. Treasury, 2022; Van Loon v. Department of the Treasury, 2024). Chainalysis 2024 documents that 2023 was a record year for the volume of money laundering through DeFi channels, with a particularly pronounced trend of chain hopping that uses DEX protocols to convert between different blockchain systems in a way that multiplies forensic complexity.

3. RANSOMWARE - CRYPTOCURRENCIES AS A BUSINESS MODEL

Ransomware, malicious software that encrypts a victim's data and demands a cryptocurrency payment for the decryption key, is not a new criminal phenomenon, but the cryptocurrency economy has transformed it from a relatively marginal tactic into an industrial criminal branch with estimated global costs of $20 billion in 2023 (Cybersecurity Ventures, 2024). This transformation is not accidental, as cryptocurrencies, particularly Bitcoin and Monero, were the factor that enabled ransomware to securely monetize its criminal operations without going through regulated financial channels. Modern ransomware operates under the Ransomware-as-a-Service (RaaS) model, in which malware creators license their tools that carry out the attacks and share the proceeds. Groups like LockBit, ALPHV/BlackCat, Clop, and Royal operate as sophisticated business entities with a victim portal, technical support for ransom negotiations, and sophisticated cryptocurrency laundering infrastructure. The FBI, CISA, and

Europol dismantled the LockBit infrastructure in a coordinated operation in February 2024, seizing 34 servers and identifying the lead operators, while explicitly warning that the RaaS system has the capacity for rapid reconstitution (FBI/NCA, 2024).

The DarkSide ransomware group's attack on Colonial Pipeline in May 2021, which caused a temporary suspension of fuel deliveries to the eastern US and a $4.4 million ransom payment in Bitcoin, was a paradigmatic example that demonstrated the ransomware ecosystem's ability to disrupt critical infrastructure and extort payments of an unprecedented volume (DOJ, 2021). Equally indicative as the attack itself was the subsequent partial recovery of the funds, as the FBI was able to trace and seize $2.3 million worth of Bitcoin, which demonstrated both the capabilities and limitations of blockchain forensics, since the remainder remained unseized (DOJ, 2021).

4. LAZARUS GROUP

A ransomware system, however sophisticated as a criminal industry, remains in the domain of profit-motivated private criminal enterprise, organized horizontally through affiliate networks, and subject to classic criminal prosecution mechanisms. The North Korean hacking group Lazarus Group represents a qualitatively different phenomenon that requires a separate analytical category, because here the state is not a regulatory actor pursuing financial crime, but is itself the immediate perpetrator of cryptocurrency heists whose proceeds finance a weapons of mass destruction program. This inversion of normative roles, where the state as a criminal actor uses cryptocurrencies to circumvent international sanctions, represents perhaps the most serious challenge that the cryptocurrency system has posed to the international security architecture to date.

The Lazarus Group operates under the umbrella of the General Bureau of Reconnaissance (RGB), a North Korean intelligence agency, and has been identified as responsible for a series of cyber operations that have far surpassed the capabilities of private criminal organizations in terms of the amount of funds seized. Chainalysis (2024) estimates that the Lazarus Group stole cryptocurrencies worth between $3 and $4 billion, an amount that is equivalent in size to the annual gross domestic product of several smaller countries and that the UN Security Council directly links to the financing of North Korea’s ballistic and nuclear programs (UN Security Council, 2024). This figure is not speculation, but the result of years of blockchain forensics conducted in parallel by Chainalysis, the US Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and UN Security Council teams.

The Lazarus Group has also developed an operational methodology that is distinctively different from the ransomware model in one key feature, which is that the group does not extort, it steals directly, through technical exploits of blockchain infrastructure whose sophistication reflects state intelligence capabilities, not individual hacking skills. The attack on Ronin Network, a blockchain bridge supporting the popular game Axie Infinity, was carried out in March 2022, resulting in the theft of $625 million worth of cryptocurrency, making it the largest single cryptocurrency theft in history (FBI, 2022; Chainalysis, 2022). The attack methodology demonstrated a level of sophistication that alarmed even the most experienced blockchain security analysts, as the Lazarus Group patiently compromised the network's validator nodes, five out of nine required to approve transactions, over a period of more than a year, and then in a coordinated effort authorized fraudulent payments that depleted the bridge's reserves.

The attack on Harmony Horizon Bridge in June 2022, which resulted in the withdrawal of $100 million, and the attack on Atomic Wallet in June 2023, with losses of about $35 million, showed that Ronin is not an isolated incident but part of a systemic strategy of targeting so-called blockchain bridges, i.e. infrastructure points that connect different blockchain networks and which, precisely due to the complexity of multiple validation, represent the most architecturally vulnerable segments of the cryptocurrency system (UN Security Council, 2024). This precise identification and consistent targeting of structural vulnerabilities, rather than opportunistic exploitation of accidental omissions, is a feature of an operational profile that reflects institutional, rather than individual, intelligence capacity.

Equally indicative of the modus operandi of the theft is the laundering process that the Lazarus Group applies to stolen funds, a process that in its sophistication and speed of execution exceeds the capacities of all known private criminal organizations. The FBI and Chainalysis document a multi-layered laundering infrastructure that combines Tornado Cash and related protocols for initial forensic chain breaking (used even after OFAC sanctions in 2022, which in itself illustrates the limits of jurisdictional enforcement of sanctions), as well as a series of cross-chain swap operations between Ethereum, Bitcoin, and Monero, which multiply forensic complexity and exhaust the analytical resources of researchers, and the final execution through OTC brokers operating in jurisdictions with minimal AML regulation, especially in Southeast Asia (Chainalysis, 2024; UN Security Council, 2024). The speed with which this chain is activated in some cases within hours of the theft, indicates a pre-prepared infrastructure that was not improvised reactively, but planned prospectively as an integral part of the operational architecture of the attack.

OFAC's sanctioning of Tornado Cash in 2022, motivated in part by the Lazarus Group's documented use of that protocol, demonstrated both the reach and limits of the sanctions toolkit, i.e. the sanctions also affected legitimate users who used the protocol for legitimate privacy reasons, while the North Korean hacking infrastructure relatively quickly adapted alternative laundering channels. This is not an argument against sanctions, but an argument for a systemic regulatory architecture that cannot rely solely on reactive measures aimed at individual infrastructure points.

The analytical significance of the Lazarus Group operations goes beyond the dimension of financial crime and enters the domain of international security. The 2024 UN Panel of Experts' assessments directly link the Lazarus Group's cryptocurrency revenues to the financing of North Korea's ballistic missile and nuclear weapons programs, programs that were supposed to be deprived of financial fuel by the international sanctions regime (UN Security Council, 2024). The cryptocurrency system in this context is not only an infrastructure for financial crime, it is a channel for sanctions erosion that threatens the architecture of international peace and security. This dimension requires that the regulatory debate on cryptocurrencies be taken out of the exclusively financial and legal framework and positioned as an issue of immediate interest to collective security mechanisms, including the UN Security Council, whose sanctions mechanisms have so far demonstrated limited effectiveness in the conditions of the cryptocurrency economy.

5. BETWEEN NORMATIVE AMBITION AND OPERATIONAL LIMITATIONS

The Financial Action Task Force (FATF), which sets global standards against money laundering, adopted in 2019 an extension of the so-called Travel Rule to cryptocurrency transactions, requiring Virtual Asset Service Providers (VASPs) to collect and exchange identifying information about senders and recipients for transactions above $1,000/euro, analogous to rules that have been in place for the banking sector for decades (FATF, 2019). This norm was a significant step towards regulatory normalization of cryptocurrencies, but its implementation reality has diverged dramatically from normative aspirations. The problem is not in the rule itself but in the architectural vulnerability of its reach. In 2023, the FATF estimated that global compliance with the Travel Rule is still far below the required threshold, especially in jurisdictions with low AML capacities.

The Markets in Crypto-Assets Regulation (MiCA), which entered into force in the EU in 2024, represents the most comprehensive regulatory framework for

cryptocurrency markets adopted anywhere in the world and an important step towards integrating the crypto sector into mainstream financial regulation (European Parliament, 2023). MiCA regulates the issuance of cryptocurrencies, crypto-asset service providers (CASPs), and stablecoins, establishing KYC requirements, capital adequacy, and consumer protection mechanisms. However, the analyst community is consistent in identifying a central limitation of MiCA, as the Regulation regulates centralized actors but has no effective reach over DeFi protocols that operate without an identified "service provider." The European Commission explicitly recognized this shortcoming in the MiCA text, announcing a revision that should address DeFi by 2026, but this revision comes in conditions in which the DeFi sector is growing exponentially and in which criminal actors, including state-sponsored groups such as the Lazarus Group, have already established sophisticated DeFi-based laundering infrastructures (European Commission, 2024).

6. CONCLUSION

The analysis of cryptocurrencies as an infrastructure of organized crime demonstrates that the regulatory challenge is not only a technical issue of developing better forensic tools, but also an architectural one through the issue of fundamental reflection on which principles the regulatory infrastructure of the cryptocurrency system should be built. Retrospective forensics, i.e. identifying criminal flows after they occur, is structurally inferior in conditions in which the speed of transactions is measured in minutes, in which cross-chain hopping is free and in which privacy coins offer a mathematical guarantee of forensic impenetrability. The Lazarus Group case illustrates this with particular sharpness, i.e. when the criminal actor is a state apparatus with intelligence capabilities and a pre-prepared infrastructure for money laundering, retrospective forensics always comes too late.

The solution that is emerging as promising is mandatory transparency of the origin of funds built directly into the protocol layer, modeled on the C2PA standard that equips digital media with verified metadata about the source. Such an approach, however, presupposes a radical redefinition of the fundamental tense relationship between privacy and transparency within the cryptocurrency system. This reconfiguration is not a cosmetic regulatory intervention. It touches on the very architectural logic of the system and requires that the two principles, which have so far been treated as procedurally irreconcilable, be rebalanced through a well-designed normative and technical intervention. This is a politically and normatively extremely complex issue, because legitimate arguments for the privacy of financial transactions are not unfounded. However, in a context where

cryptocurrencies are becoming the infrastructure for financing nuclear programs, ransomware attacks on hospitals, and laundering narcotics money, the question of the optimal balance between privacy and transparency must be placed at the center of democratic deliberation, and not left to be resolved "de facto" by criminal actors exploiting regulatory loopholes.

LITERATURE

1. Chainalysis, 2020. The Monero Tracing Challenge: Internal Assessment. Chainalysis Inc, https://www.chainalysis.com/blog/all-about-monero/(1.4.2026.).
2. Chainalysis, 2020. The Ronin Network Hack. Chainalysis Blog, https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/(1.4.2026.)
3. Chainalysis, 2024. The 2024 Crypto Crime Report. Chainalysis Inc., New York, https://go.chainalysis.com/crypto-crime-2024.html, (2.4.2026.)
4. Christin, N., 2013. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In Proceedings of WWW 2013. ACM.
5. Cybersecurity Ventures, 2024. Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031. Cybersecurity Ventures Annual Report. https://www.google.com/search?q=5.%09Cybersecurity+Ventures%2C+2024.+Global+Ransomware+Damage+Costs+Predicted+to+Exceed+%24265+Billion+by+2031, (3.4.2026.).
6. European Commission, 2024. Digital Finance Package: Review of MiCA and DeFi Regulatory Framework. COM(2024) 192 final.
7. European Parliament, 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). Official Journal of the EU, L 150.
8. Europol, 2023. Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol Spotlight Report, Den Haag. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies, (5.4.2026.)
9. FATF, 2019. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF/OECD, Paris.
10. FATF, 2023. Targeted Update on Implementation of FATF Standards on Virtual Assets/VASPs. FATF/OECD, Paris.
11. FBI / National Crime Agency, 2024. Operation Cronos: Disruption of LockBit Ransomware Group — Joint Press Release. https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant, (5.4.2026.).
12. FBI, 2013. Silk Road Takedown: United States v. Ross Ulbricht. DOJ Press Release, https://en.wikipedia.org/wiki/Silk_Road_(marketplace), (5.4.2026.).
13. FBI, 2022. FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Heist. Press Release,

https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft, (6.4.2026.).
14. Foley, S., Karlsen, J. R. & Putniņš, T. J., 2019. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? Review of Financial Studies, 32(5), 1798–1853, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645, (6.4.2026.).
15. IRS Criminal Investigation, 2020. IRS CI Seeks Contractors for Monero-Tracing Pilot. Solicitation Number: 2032H321R00001.
16. Intelligence from the Bitcoin Spagnuolo, M., Maggi, F. & Zanero, S., 2014. BitIodine: Extracting Network. In Financial Cryptography and Data Security, Springer. https://static.miki.it/pdf/BitIodine_presentation.pdf, (7.4.2026.).
17. Korajlić, N., Selimić, M., Trnčić, L., Sahadžić, N., 2023. "The importance of intuitively creative criminology in solving complex crimes", Protection and Security, year 3, issue 2, www.zisjournal.com.
18. Möser, M., Soska, K., Heilman, E. & Lee, K., 2018. An Empirical Analysis of Traceability in the Monero Blockchain. In Proceedings of the Workshop on Bitcoin Research. https://www.researchgate.net/publication/324863990_An_Empirical_Analysis_of_Traceability_in_the_Monero_Blockchain, (7.4.2026.).
19. Muhić, E., 2024. "Operational use of OSINT in the investigation of organized criminal groups" Protection and Security, year 4, issue 2, www.zisjournal.com.
20. U.S. Department of Justice, 2021. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide. DOJ Press Release, (7.4.2026.).
21. U.S. Department of the Treasury – OFAC., 2022. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Press Release, (7.4.2026.).
22. UN Security Council. (2024). Final Report of the Panel of Experts on North Korea, S/2024/215. United Nations, New York.
23. Van Loon v. Department of the Treasury, 2024., No. 23-50669 (5th Cir. 2024), https://law.justia.com/cases/federal/appellate-courts/ca5/23-50669/23-50669-2024-11-26.html, (8.4.2026.).