HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 3. szám 25–48.
DOI: 10.32567/hm.2025.3.2

Benke Bálint Péter[1]

A kriptovaluták kettős arca

A kriptovaluták által nyújtott technológiai innovációk szerepe a kiberbűncselekményekben, 1. rész

The Dual Nature of Cryptocurrencies

The Impact of Technological Innovations behind Cryptocurrencies on Cybercrime, Part 1

Absztrakt

A digitális világ dinamikus fejlődése alapjaiban alakította át a pénzügyi tranzakciók működését, amelyben a kriptovaluták megjelenése új korszakot nyitott. Az olyan decentralizált eszközök, mint a Monero, Zcash és Dash lehetővé teszik az anonim és gyors pénzmozgásokat, komoly kihívások elé állítva a hagyományos ellenőrzési mechanizmusokat. Bár e technológiák számos előnyt hordoznak, jelentős biztonsági kockázatokat is rejtenek. Anonimitásuk és szabályozatlanságuk különösen vonzóvá teszi őket a bűnözők számára pénzmosás, csalás, zsarolóvírus-támadások és terrorizmusfinanszírozás céljára. A dark web piacterei tovább erősítik ezen eszközök illegális felhasználását azáltal, hogy anonim hozzáférést biztosítanak illegális szolgáltatásokhoz, jelentősen megnehezítve a bűnüldöző szervek munkáját. A tanulmánysorozat első része a releváns tudományos és szakirodalom feldolgozásán, valamint esettanulmányok elemzésén keresztül ad áttekintést a témáról. A második rész empirikus kutatásra támaszkodva vizsgálja a rendvédelmi szervek gyakorlati tapasztalatait a kriptovalutákhoz kötődő bűncselekményekkel kapcsolatban.

Kulcsszavak: kiberbűnözés, kriptovaluta, privacy coin, bűnüldözés, anonimitás

[1] Okleveles kiberbiztonsági és nemzetközi biztonság- és védelempolitikai szakértő, e-mail: benke.balint@proton-mail.com

Abstract

The dynamic evolution of the digital world has fundamentally transformed the nature of financial transactions, ushering in a new era with the emergence of cryptocurrencies. Decentralised assets such as Monero, Zcash, and Dash enable fast and anonymous transfers, posing significant challenges to traditional regulatory mechanisms. While these technologies offer several benefits, they also entail serious security risks. Their anonymity and lack of oversight make them particularly attractive to criminals for activities such as money laundering, fraud, ransomware attacks, and terrorism financing. Dark web marketplaces further amplify their illicit use by facilitating anonymous access to illegal services, significantly complicating the work of law enforcement agencies. The first part of the study series provides an overview of the topic through the analysis of relevant scientific and professional literature, as well as case studies. The second part builds on empirical research to examine the practical experiences of law enforcement agencies regarding crimes related to cryptocurrencies.

Keywords: cybercrime, cryptocurrency, privacy coin, law enforcement, anonymity

Bevezetés

A pénz fogalmának értelmezése a 21. századra jelentős átalakuláson ment keresztül, amelynek egyik legmarkánsabb megnyilvánulása a blokkláncalapú, digitális fizetőeszközök – azaz kriptovaluták – elterjedése. Ezen eszközök közül külön figyelmet érdemelnek az úgynevezett privacy coin[2]-ként kategorizált valuták (például monero, zcash, dash), amelyek működésükből fakadóan fokozott anonimitást biztosítanak a tranzakciók során. Ezek a technológiai megoldások megnehezítik a pénzügyi felügyeleti szervek számára a tranzakciók ellenőrzését és visszakövetését.

Az Európai Unió több jogalkotási megoldással igyekszik reagálni a kriptoeszközök által támasztott pénzügyi és bűnüldözési kihívásokra. A legfrissebb 2024-es szabályozás, a 6. pénzmosás elleni irányelv (AMLD6) már kifejezetten nevesíti a kriptoeszközöket mint pénzmosásra alkalmas vagyonformát, és kötelező regisztrációs, valamint ügyfél-azonosítási kötelezettséget ír elő a kriptotőzsdék és tárcaszolgáltatók számára. Az irányelv egyúttal külön büntetőjogi státuszt biztosít a pénzmosásnak mint önálló bűncselekménynek, kiterjesztve a büntethetőséget a segítő személyekre, a pénzmosásból származó javak átruházóira, valamint a jogi személyek felelősségére is.[3]

A 2023-ban elfogadott Markets in Crypto-Assets Regulation (MiCA), valamint a vele párhuzamosan bevezetett Anti-Money Laundering Regulation (AMLR) célja a kriptoeszközök piacának átláthatóvá tétele, a fogyasztóvédelem erősítése, továbbá

[2] A *privacy coinok* olyan kriptovaluták, amelyeket kifejezetten a tranzakciók anonimitására és a felhasználók adatainak védelmére terveztek. Ezek a kriptovaluták, mint például a monero vagy a zcash speciális kriptográfiai technikákat alkalmaznak (mint a *ring signature* vagy zk-SNARK), hogy elrejtsék a tranzakciós felek címét, az összegeket és a tranzakciók láncolatát.

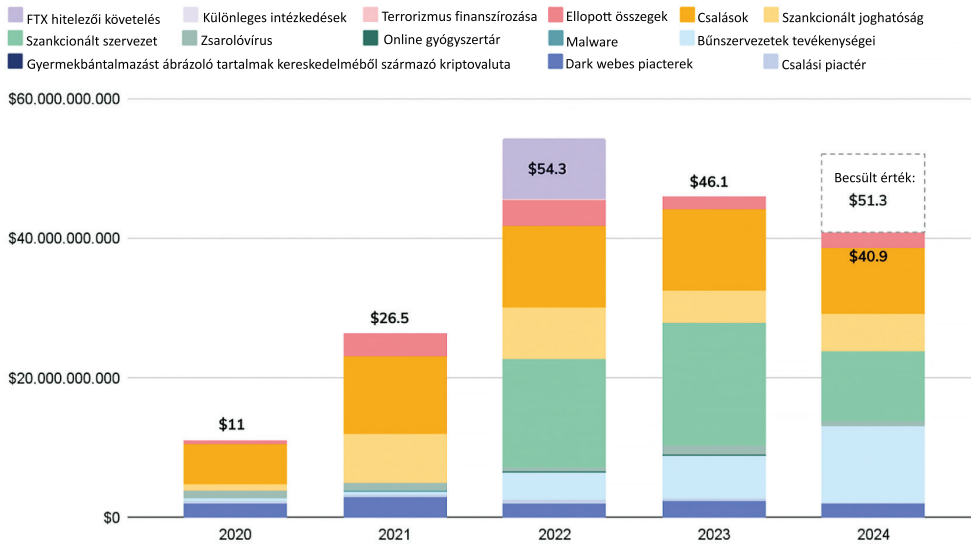
[3] Az Európai Unió és a Tanács (EU) 2024/1640 irányelve.

a pénzmosás megelőzése.[4] A szabályozási törekvések azonban nemcsak európai szinten jelennek meg. A nemzetközi szervezetként működő Pénzügyi Akciócsoport (FATF) a kriptoeszközökkel kapcsolatos pénzmosás és terrorizmusfinanszírozás-ellenes szabályok kialakításában is szerepet vállal. Az FATF 2019-es ajánlásai értelmében a kriptoeszköz-szolgáltatókra ügyfélazonosítási és tranzakciókövetési kötelezettségek vonatkoznak. Ezek közül kiemelkedik a Travel rule elnevezésű előírás, amely szerint a kriptoeszközök továbbításakor a tranzakcióban részt vevő felek adatait is rögzíteni kell. Az ilyen ajánlások világszerte alapul szolgálnak a nemzeti szabályozások kialakításához.[5]

A felsorolt jogszabályi normák hatálya ugyanakkor elsősorban a centralizált, illetve a hagyományos webes felületeken működő kriptotőzsdékre és szolgáltatókra terjed ki. Az olyan decentralizált vagy anonimitásra épülő megoldások, mint a privacy coinokat támogató rendszerek vagy a dark weben működő escrow (letéti) platformok technológiai sajátosságaik révén kívül esnek az intézményesített felügyelet hatókörén, így ezek ellenőrizhetősége továbbra is korlátozott. Ahogy a kriptovaluták egyre szélesebb körben ismertté és hozzáférhetővé válnak, a felhasználók körében egyre erősebben megjelenik a kimaradástól való félelem (FOMO[6]) érzése is, ami jelentősen hozzájárul a felhasználói bázis gyors bővüléséhez. Ez a növekedés azonban nemcsak a pénzügyi és technológiai fejlődést támogatja, hanem sok laikus felhasználója is lesz az ilyesfajta vagyonelemeknek, ami párhuzamosan együtt jár azzal is, hogy a kriptovaluták bűncselekményekhez való felhasználása is fokozódik, kiemelten a csalások terén.

A kriptovaluták előnyei – mint a pénzügyi szabadság, az adatvédelem vagy a globális hozzáférés – vitathatatlanok, ugyanakkor fennáll a veszélye, hogy ugyanezek az eszközök visszaélésekre, csalásokra, pénzmosásra és kiberbűncselekmények támogatására is felhasználhatók. Az elmúlt években drasztikusan nőtt azoknak a kriptovaluta-összegeknek a mennyisége, amelyeket jogellenes tevékenységekhez kötöttek. A Chainalysis 2025-ös Crypto Crime Reportja szerint például 2022 óta jelentős mértékben emelkedett az illegális célokra felhasznált digitális eszközök aránya, amint az az 1. ábrán látható. Az illegális tranzakciók azonosítása és visszakövetése rendkívül komplex, idő- és erőforrás-igényes feladat a bűnüldöző hatóságok számára. A helyzet súlyosságát fokozza, hogy ezeknek a szervezeteknek nemcsak a gyorsan változó technológiai környezettel, hanem az egyre felkészültebb bűnelkövetőkkel is versenyt kell futniuk.

[4] Az Európai Unió és a Tanács (EU) 2023/1114 rendelete; Az Európai Unió és a Tanács (EU) 2024/1624 rendelete.
[5] FATF 2021.
[6] A FOMO *(fear of missing out),* vagyis a kimaradástól való félelem egy pszichológiai jelenség, amely során az egyén szorongást él át attól tartva, hogy lemarad valamilyen számára előnyös vagy népszerű eseményről, lehetőségről. A kriptovaluták világában ez gyakran ösztönöz impulzív befektetési döntéseket a hirtelen árfolyamemelkedések vagy piaci trendek hatására.



1. ábra: A bűncselekményekhez köthető kriptovaluta-tranzakciók becsült éves összértékének alakulása 2020 és 2024 között, milliárd dollárban

Megjegyzés: Az adatok a vizsgált időszakban folyamatos növekedést mutatnak, 2022-ben érve el a csúcsot (54,3 milliárd USD), majd 2023-ban kisebb visszaesés következett be (46,1 milliárd USD). A 2024-es becslés (51,3 milliárd USD) arra utal, hogy a piac részben visszanyerte korábbi szintjét. A változások hátterében jelentős események – például a Hydra Market 2022-es bezárása – álltak, amelyek szerkezeti átrendeződést és új szereplők megjelenését eredményezték.

Forrás: a szerző szerkesztése Chainalysis 2025 alapján

A fentiek alapján megállapítható, hogy a kriptovaluták köztudatban és gazdaságban való elterjedése, valamint azok anonimitást biztosító technológiai sajátosságai komoly kihívás elé állítják a jogalkalmazó szerveket, különösen a bűncselekmények nyomozásának és a pénzügyi visszaélések felderítésének területén. Az anonim tranzakciók térnyerése elősegíti, hogy a kriptovaluták a kiberbűnözés, pénzmosás, csalás vagy éppen zsarolóvírusos támadások eszközeivé váljanak. Ennek hátterében olyan technikai megoldások állnak, mint a coin mixerek, a decentralizált tőzsdék vagy az úgynevezett privacy coinok, amelyek jelentősen megnehezítik a tranzakciók visszakövethetőségét és a bűnelkövetők azonosítását.

Ebből fakadóan e tanulmány kutatási célkitűzései az alábbiak szerint foglalhatók össze:

1. Feltérképezni, hogy mely kriptovalutákat használják leggyakrabban bűnelkövetések során.
2. Bemutatni és elemezni azokat a technikákat és módszereket, amelyeket a bűnözők a kriptovaluta-tranzakciók elrejtésére és a visszakövetés megnehezítésére alkalmaznak.
3. Azonosítani a kriptovalutákhoz kapcsolódó leggyakoribb bűncselekménytípusokat és azok jellemzőit.

A kutatás során az alábbi kérdésekre kerestem választ:

1. Mely kriptovaluták a leggyakoribb eszközei a különböző típusú bűncselekményeknek?
2. Milyen technológiai eszközökkel és módszerekkel igyekeznek a bűnelkövetők eltüntetni vagy elrejteni a kriptovaluta-tranzakciók nyomait?

A fenti szempontok alapján a kutatáshoz az alábbi hipotéziseket fogalmaztam meg:

H1: A bitcoin továbbra is a leggyakrabban alkalmazott kriptovaluta a kiberbűnözésben, azonban a privacy coinok és az ethereum szerepe növekszik, ami új bűnügyi trendek és kihívások megjelenéséhez vezet.

H2: A kriptovalutákkal kapcsolatos bűncselekmények elkövetői folyamatosan alkalmazzák az anonimizálást és a visszakövethetőség akadályozását szolgáló technológiákat – például coin mixereket, privacy coinokat és decentralizált tőzsdéket –, ami változó és összetett kihívást jelent a bűnüldöző hatóságok számára.

Módszertan

A tanulmány kvalitatív módszertani elemeket alkalmaz, kombinálva az elméleti és az esettanulmány-alapú megközelítéseket. A kutatás első szakaszában szisztematikus szakirodalmi áttekintést végzek, amelynek célja a kriptovalutákhoz köthető bűncselekménytípusok, a kapcsolódó technológiai eszközök, valamint azok bűnügyi relevanciájának feltérképezése volt.

A szakirodalmi keresés során a Scopus és IEEE Xplore adatbázisok szolgáltak elsődleges forrásként. A keresések során alkalmazott kulcsszó-kombinációk a következők voltak: „cryptocurrency AND cybercrime", „privacy coin AND money laundering", „cryptocurrency AND ransomware", „cryptocurrency AND dark web". A találatok szűrése relevancia, szakmai elismertség (Scimago Journal Rank Q1 – Q2 besorolás), valamint publikációs aktualitás alapján történt. Az elméleti keret kiegészítéseként bevontam olyan szakmailag elismert, nem lektorált, de megbízható forrásokból származó jelentéseket, elemzéseket és hírközléseket is, különösen a Chainalysis és TRM Labs publikációit, amelyek az aktuális fejleményekről gyakran a tudományos közléseket megelőzően számolnak be.

A kvalitatív módszertani részben célzott mintavétellel kiválasztott esettanulmányokat elemeztem. A válogatás szempontját az adott fejezetek tematikus fókuszához való illeszkedés, valamint az a cél jelentette, hogy az esetek a szakirodalomban leírt elméleti kategóriákat szemléletesen illusztrálják, és hozzájáruljanak a kriptovaluta-alapú bűncselekmények gyakorlati kontextusának jobb megértéséhez. A kiválasztás további meghatározó szempontja az volt, hogy az esettanulmányok hazai jelentőségűek legyenek, mint például az UNIX Autó Kft.-t ért zsarolóvírus-támadás, vagy a nemzetközi színtéren a legjelentősebb ügyek közé sorolhatók legyenek, mint a Bitconnect csalási eset vagy Colonial Pipeline elleni zsarolóvírus-támadás.

A kvantitatív adatok a Chainalysis *Crypto Crime Report* 2024-es és 2025-ös kiadásain alapulnak, amelyek megbízható és naprakész statisztikai információkat szolgáltatnak a kriptovalutákhoz köthető bűncselekmények volumenére, típusaira és dinamikájára vonatkozóan.

A tanulmány felépítése az IMRAD módszert követi, amely magában foglalja a bevezetést, a kutatási módszertant, az eredmények fejezetet és a diszkussziót. A bevezetés ismerteti a kutatás hátterét és célkitűzéseit, a módszertan fejezet részletezi az alkalmazott kutatási eljárásokat, míg az eredmények rész bemutatja a kriptovalutákkal kapcsolatos bűncselekménytípusok főbb fajtáit és jellemzőit. A diszkusszió fejezet a hipotézisek vizsgálatának eredményeit tézisszerűen összegzi, majd ezek értelmezésével és kifejtésével betölti a záró következtetések fejezet funkcióját.

A módszertani kialakítás célja nem pusztán a kriptovalutákhoz köthető bűncselekménytípusok katalogizálása volt, hanem a mögöttes mintázatok azonosítása és értelmezése is, különös tekintettel a szabályozási és bűnüldözési kihívások gyakorlati vetületeire. A tanulmány egy két részből álló cikksorozat első része. A folytatás olyan interjúalapú kvalitatív és kvantitatív elemzéseket mutat be, amelyek kifejezetten a rendvédelmi szervek gyakorlatára és tapasztalataira összpontosítanak.

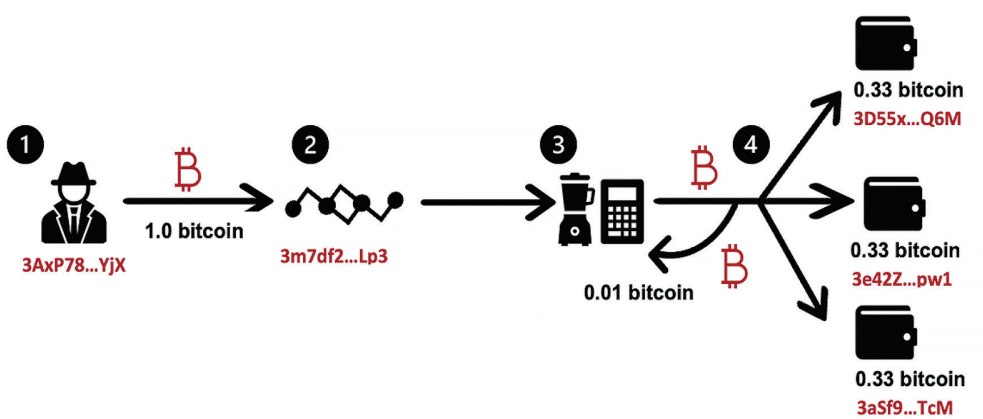
Alapfogalmak

A kriptovaluta olyan digitális fizetőeszköz, amely nem rendelkezik fizikai megjelenési formával, így eltér a hagyományos valutáktól, mint például az érmék vagy a bankjegyek. Működése kriptográfiai módszereken alapul, és decentralizált technológiai infrastruktúrákra, elsősorban blokkláncalapú hálózatokra épül. A hálózatok lehetővé teszik a biztonságos, ellenőrizhető és transzparens tranzakciók lebonyolítását anélkül, hogy központi hatóság vagy pénzügyi közvetítő beavatkozására lenne szükség.[7] A blokklánc-technológia alapegysége a blokk, amely strukturált formában tartalmazza a tranzakciós adatokat. Minden blokk egy adott időintervallumban végrehajtott tranzakciók összesítését reprezentálja, továbbá tartalmazza az előző blokk kriptográfiai hasítóértékét (hash), amely biztosítja a láncolat folytonosságát és integritását. Ez a megoldás lehetővé teszi, hogy a blokkok időrendi sorrendben kapcsolódjanak egymáshoz, és így egy visszamenőlegesen nem módosítható, elosztott főkönyv jöjjön létre. A blokklánc mint technológiai rendszer decentralizált környezetben működik, ahol minden résztvevő (node) másolatot tárol a teljes tranzakciós előzményről. A rendszer alapvető jellemzője, hogy a rögzített információk transzparensek, nyilvánosan hozzáférhetők és utólagos módosításra gyakorlatilag nem alkalmasak, mivel bármely változtatás érvénytelenné tenné az utána következő blokkok hasítóértékeit. Ez a struktúra egy olyan biztonságos és megbízható adatbázist eredményez, amelyben a tranzakciók hitelesítése konszenzusalapú mechanizmusok révén történik, központi ellenőrzés nélkül.[8]

[7] Nakamoto 2008.
[8] Mukhopadhyay et al. 2016.

A kriptovaluták tranzakcióinak nyomon követhetőségét jelentősen megnehezíti a különféle anonimizáló technológiák alkalmazása. Az egyik legelterjedtebb eszköz ebben a körben a coin mixer (más néven coin tumbler) szolgáltatás, amely a blokkláncon végzett pénzmozgások forrásának és céljának összekapcsolását hivatott obfuszkálni. Jelen tanulmányban a coin mixer terminust használjuk. A coin mixer szolgáltatások működési elve azon alapul, hogy a felhasználók kriptovalutát juttatnak el a keverési platformra, ahol az adott összegeket más felhasználók tranzakcióival együttesen dolgozzák fel. Az így kialakuló kriptovaluta halmazából újbóli szétosztása során a rendszer a címzettek részére olyan új tranzakciókat hoz létre, amelyek nem tartalmaznak közvetlen kapcsolatot az eredeti forráshoz. Ezzel a módszerrel a küldő és a végső címzett közötti összefüggés megszakad vagy jelentősen obfuszkálódik, így a tranzakciók visszafejtése és nyomon követése blokkláncelemzéssel nagyban megnehezül.[9] Egyik legismertebb platform a Samourai Wallet nevű Bitcoin mixer volt, amelyet 2015-ben hoztak létre azzal a céllal, hogy pénzügyi anonimitást biztosítson felhasználóinak. A szolgáltatás működése azonban 2024-ben jelentős figyelmet kapott, amikor az alapítókat pénzmosással kapcsolatos összeesküvés vádjával letartóztatták.[10]

A kiberbűnözés elleni fellépés során jelentős strukturális kihívást jelent az erőforrásbeli aszimmetria a bűnözői szereplők és a bűnüldöző hatóságok között. A rendelkezésre álló eszközök és technológiák költséghatékonysága gyakran a bűnelkövetők oldalán jelent előnyt, mivel az általuk használt szolgáltatások olcsóbbak és rugalmasabbak, mint azok a komplex megoldások, amelyeket a hatóságok kénytelenek alkalmazni. Emellett egyes szervezett bűnözői hálózatok olyan mértékű anyagi forrásokkal rendelkeznek, amelyek lehetővé teszik számukra fejlett technikai infrastruktúrák kiépítését és működtetését, időnként meghaladva az állami szereplők technológiai lehetőségeit.



2. ábra: A kriptovaluta-keverés folyamata lépésről lépésre
Forrás: a szerző szerkesztése Intel 471 2021 alapján

[9] Mariani–Homoliak 2025.
[10] Southern District of New York 2025.

A 2. ábra vizuálisan szemlélteti, hogyan működik egy tipikus kriptovalutamixer-szolgáltatás:

1. lépés: A kiberbűnöző kriptovalutát küld egy mixerszolgáltatás által megadott kriptovaluta-tárca[11] címre.

2. lépés: Az utalt összeg bekerül a mixerszolgáltatás platformjára, ahol más felhasználóktól származó kriptovalutákkal, valamint a szolgáltató saját tartalékaival keveredik össze.

3. lépés: A rendszer egy kriptográfiai keverő algoritmust alkalmaz, amelynek célja a tranzakciós nyomvonal obfuszkálása. Ebben a fázisban továbbá a szolgáltatás levonja a működtetéséért járó jutalékot is.

4. lépés: A „megtisztított" összeget visszautalják a kiberbűnöző által megadott, többnyire újonnan létrehozott tárcacímekre, ezzel megnehezítve az eredeti forrás azonosítását.[12]

Nem minden kriptovaluta esetében szükséges külső keverési szolgáltatás igénybevétele, mivel egyes kriptovaluták, például a monero, zcash vagy dash natívan beépített anonimizációs megoldásokat alkalmaznak. A Monero működésének alapját a CryptoNote protokoll képezi, amelyet kifejezetten a tranzakciók visszakövethetetlenségének és a felhasználói anonimitásnak a biztosítására fejlesztettek. A protokoll három anonimitást biztosító technológiát integrál:

- Stealth addresses (védett címek): minden tranzakcióhoz egyedi, egyszer használatos cím generálódik, így a címzett személye nem köthető össze a publikus címmel.
- Ring signatures (gyűrűaláírások): az aláíró nyilvános kulcsát egy véletlenszerűen kiválasztott csoport kulcsai közé „rejti el", megnehezítve a küldő egyértelmű azonosítását.
- Ring Confidential Transactions (RingCT): a tranzakciók összegeit titkosítja, így sem az összeg, sem a küldő és fogadó fél kiléte nem rekonstruálható.[13]

A felsorolt technológiai megoldások révén a Monero jelenleg az egyik legfejlettebb anonimitást biztosító kriptovalutának tekinthető.[14]

Érdemes kiemelni, hogy ezzel szemben a Bitcoin egy pszeudoanonim fizetési rendszernek tekintendő, mivel a tranzakciók során a felhasználók valós személyazonossága helyett kriptográfiai címeket használnak. Ezek a Bitcoin-címek álvéletlenszerűen generálódnak egy adott matematikai algoritmus alapján, így minden cím egyedi és látszólag véletlenszerű. Ez a megoldás bizonyos fokú anonimitást kínál, ugyanakkor nem teszi lehetővé a teljes rejtettséget. Mégis, a felhasználóknak lehetőségük van arra, hogy minden egyes tranzakcióhoz új címet hozzanak létre. Ezzel a gyakorlattal csökkenthető annak az esélye, hogy egyetlen cím alapján átfogó képet lehessen alkotni az adott felhasználó pénzügyi tevékenységéről. Bár a címek kriptográfiai alapokon nyugszanak, és visszafejtésük

[11] A kriptovaluta-tárca olyan digitális fizikai eszköz vagy szoftver, amely lehetővé teszi a felhasználók számára, hogy privát és nyilvános kulcsokat hozzanak létre, tároljanak, és ezek segítségével biztonságosan kezeljék kriptovalutáikat, valamint lebonyolítsák blokkláncalapú tranzakcióikat. A kriptovaluta-tárcák fő típusai a szoftveres (asztali, online, mobil), valamint a hardveres tárcák, amelyeken belül megkülönböztetünk forró (internetes) és hideg (offline) tárolási megoldásokat.

[12] Intel 471 2021.

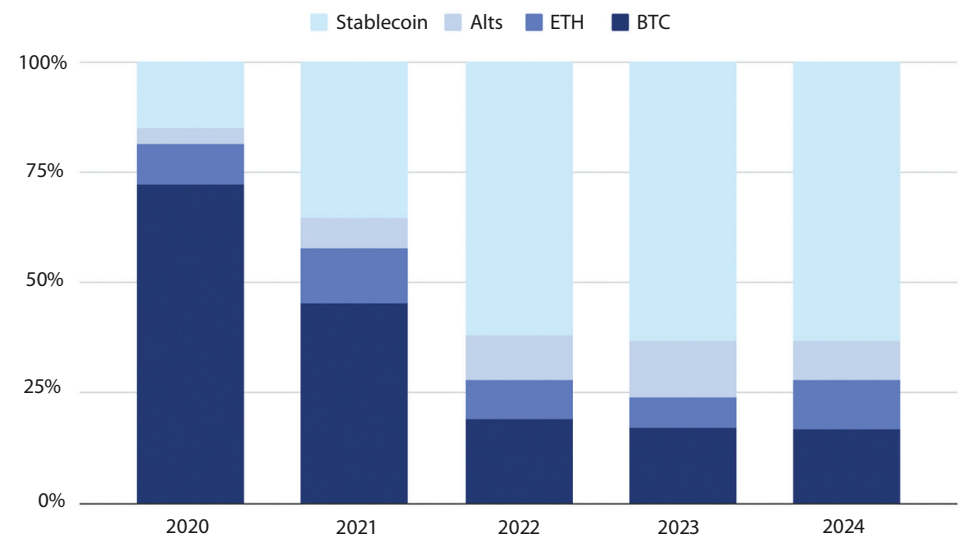
[13] Monero 2024.

[14] Noether 2015; Li et al. 2021.

jelentős technikai kihívást jelent, megfelelő elemzőeszközök és metaadatok segítségével bizonyos esetekben mégis azonosíthatók a felhasználók.[15]

A Chainalysis 2025-ös Crypto Crime Reportja megállapításai szerint továbbra is a bitcoin a leggyakrabban használt kriptovaluta bűncselekmények elkövetése során. Ennek oka elsősorban a bitcoin széles körű ismertsége, elterjedtsége, valamint az, hogy a legtöbb kriptovalutát elfogadó platform alapértelmezés szerint ezt tekinti elsődleges fizetőeszköznek. A 3. ábra alapján ugyanakkor megfigyelhető, hogy a tranzakciók bűnözéshez kapcsolható összértékének jelentős hányadát már az úgynevezett stablecoinok[16] teszik ki, mint például az USDC, USDT vagy EUROC. Míg a Bitcoin tranzakcióinak megerősítése időigényes lehet, a stablecoinok gyakorlatilag azonnali átutalást tesznek lehetővé. Ezenfelül stabil árfolyamuk miatt különösen alkalmassá válnak nagy volumenű pénzmozgások lebonyolítására, mivel minimalizálják az árfolyam-ingadozásokból eredő kockázatot.

Fontos azonban megjegyezni, hogy noha a stablecoin transzferek aggregáltan kiemelkedők, ezek több különböző kriptovalutát foglalnak magukban, így nem értelmezhetők egyetlen kriptovalutaként a használati gyakoriság szempontjából. A 3. ábra további adataiból kiolvasható tendencia az ethereum növekvő szerepe a bűncselekményekhez köthető tranzakciók terén, amely az ökoszisztéma technológiai sokszínűségével és a decentralizált pénzügyi (DeFi)[17] protokollok integrációjával magyarázható.



3. ábra: Bűncselekményekhez kapcsolódó tranzakciók eloszlása kriptovaluta-típusok szerint (2020–2024)
Forrás: a szerző szerkesztése Chainalysis 2025 alapján

[15] Zhang et al. 2020.

[16] A *stablecoinok* olyan kriptovaluták, amelyek értéküket egy stabil árfolyamú gazdasági eszközhöz (pl. amerikai dollár, euró vagy arany) kötik annak érdekében, hogy elkerüljék a kriptopiacra jellemző volatilitást.

[17] A decentralizált pénzügyi (DeFi) protokollok olyan blokkláncalapú alkalmazások, amelyek központi pénzügyi közvetítők (pl. bankok, brókerek) nélkül teszik lehetővé pénzügyi műveletek lebonyolítását. Ezek az okosszerződésekre épülő rendszerek átlátható módon működnek, de gyakran névtelenül használhatók, így a szabályozás és ellenőrzés szempontjából komoly kihívást jelentenek.

Meglepő módon a kifejezetten anonimitásra épülő privacy coinok, amelyek az altcoinok körébe tartoznak (például Monero), a Chainalysis adatai alapján mindössze marginális arányban fordulnak elő az illegális tranzakciók teljes volumenében.[18]

Pénzmosás

A bűncselekménytípusok vonatkozásában a pénzmosás az egyik legfontosabb, amelynek elősegítésében szerepet játszanak a kriptovaluták. A pénzmosás olyan többlépcsős folyamat, amelynek célja, hogy a jogellenes forrásból származó bevételeket – például drogkereskedelemből, csalásból vagy korrupcióból eredő jövedelmeket – látszólag legális eredetű jövedelemmé alakítsák. Ennek eredményeként az illegális tőke problémamentesen visszaáramolhat a formális gazdaságba, a hatósági ellenőrzés elkerülésével.[19]

A pénzmosás folyamata a szakirodalomban hagyományosan három egymást követő szakaszra tagolódik (4. ábra):

1. Elhelyezés

Az első fázisban az illegális forrásból származó jövedelmet bevezetik a hivatalos pénzügyi rendszerbe, jellemzően banki befizetések, pénzváltások, tárgyak vásárlása vagy digitális eszközök – például kriptovaluták, NFT-k – vásárlása útján. Ebben a fázisban a legmagasabb annak a kockázata, hogy a pénzmosás lelepleződik.

2. Rétegzés

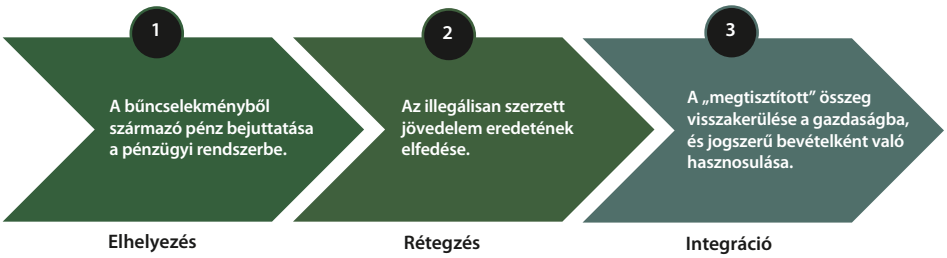
A második szakasz során a bűnözők többszörös tranzakciós műveletekkel igyekeznek eltüntetni az eredeti jövedelem nyomait. Ekkor gyakori a tőke különböző kriptovalutákba történő átváltása, coin mixerek vagy DeFi protokollok használata, valamint a pénzeszközök különböző országokon keresztül történő mozgatása. A folyamat során jelentős mértékben megnő a tranzakciók száma, mivel az elkövetők ismétlődő átutalásokkal és összetett pénzmozgásokkal igyekeznek a tranzakciós láncot széttagolni és a nyomon követhetőséget csökkenteni.

3. Integráció

Az utolsó fázisban a megtisztított vagyon visszakerül a formális gazdasági rendszerbe. Ez például ingatlanvásárlás, üzleti befektetés vagy más pénzügyi művelet révén

[18] Chainalysis 2025.
[19] Levi 2002.

valósulhat meg. Az integráció gyakran olyan országokban történik, amelyek kedvező pénzügyi szabályozást kínálnak – ezek az úgynevezett adóparadicsomok.[20]



4. ábra: A pénzmosás három szakasza kriptovalutákkal

Megjegyzés: Az illegális forrásból származó kriptovaluták elhelyezése után a rétegzés során kriptovaluta-keverők és privacy coinok alkalmazásával rejtik el a forrását, majd az integrálás során a „megtisztított" összegeket fiat valutára váltják vagy közvetlenül felhasználják

Forrás: a szerző szerkesztése Schneider–Windischbauer *2008 alapján*

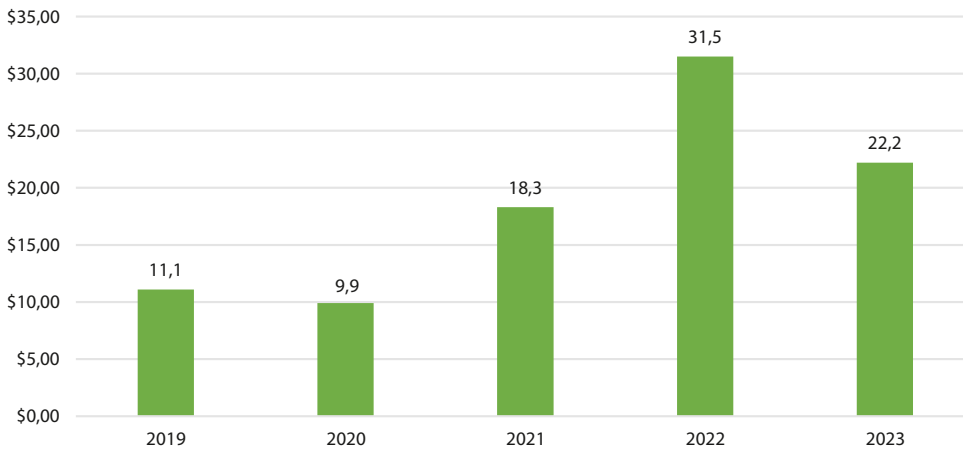
Az utóbbi években a bűnözők forradalmasították a pénzmosás folyamatát a kriptovaluták révén, hogy elkerüljék a szabályozó hatóságok ellenőrzését. A kriptovaluták megjelenése előtt a bűnözők kénytelenek voltak illegális módon szerzett kriptovalutáikat a központi bankrendszeren keresztül mozgatni és elrejteni. Ennek következtében különböző kormányok képesek voltak közvetett módon ellenőrizni a pénzmosást azáltal, hogy szigorúbb szabályozásokat és nagyobb bírságokat róttak ki a bankokra és pénzintézetekre, ami egyre nehezebbé tette az illegális tőkék mozgatását. Ezzel szemben, mivel a kriptovaluták nem igényelnek központi banki közreműködést, képesek teljesen megkerülni a hagyományos bankrendszert. A kriptovaluták további gazdasági ösztönzőket biztosítanak a bűnözők számára, így még vonzóbbá téve számukra ezt a rendszert. Az egyik növekvő előny számukra az, hogy a kriptovaluták egyre szélesebb körben elfogadott fizetőeszközként jelennek meg az áruházláncok és kereskedők körében. Jelenleg ez az elfogadottság még korlátozott, mivel a kriptovalutákat gyakran át kell váltani hagyományos, fiat pénznemekre.[21] Egy másik, még meghatározóbb előnye a kriptovaluták használatának, hogy rendkívül könnyen lehet velük pénzt mozgatni egyik országból a másikba. A pénzmosás rétegzési szakaszában az illegális úton szerzett összegeket nemcsak számos pénzügyi tranzakció lebonyolítására használják, hanem más pénzügyi joghatóságokba is átutalják, ahol a bűnelkövetők könnyen hozzáférhetnek forrásaikhoz, ezáltal védve vagyonukat a lefoglalás ellen. A kriptovaluták pénzmosásban betöltött szerepének növekedését jól szemlélteti az 5. ábra, amely az éves kriptovaluta-pénzmosási összegek alakulását mutatja be 2019 és 2023 között, milliárd amerikai dollárban kifejezve.[22]

[20] Schneider–Windischbauer 2008.

[21] A fiat pénz olyan hivatalos fizetőeszköz, amelyet az állam bocsát ki, és amelynek értékét nem valamilyen mögöttes termék – például arany vagy ezüst – biztosítja, hanem az adott ország kormányába és gazdaságába vetett bizalom. Ez azt jelenti, hogy azért fogadjuk el fizetésként, mert a törvény érvényes fizetőeszközként ismeri el, és mert bízunk benne, hogy stabilan megőrzi az értékét.

[22] Albrecht et al. 2019.

Amennyiben európai uniós szemszögből vizsgáljuk a kriptovaluták és a pénzmosás jogi szabályozását, rendkívül fontos az Európai Parlament és a Tanács 2024/1624 (AMLR) rendelete, amely a pénzügyi rendszer pénzmosás vagy a terrorizmus finanszírozása céljára történő felhasználásának megelőzését hivatott szolgálni. A rendelet többek között előírja a kriptovaluta-szolgáltatók számára az ügyfél-azonosítási (KYC[23]) kötelezettségek szigorítását, tiltja az anonimizáló eszközök alkalmazását, mint például a coin mixereket, illetve a privacy coinokat, mint a Monero, Zcash vagy Dash.[24]



5. ábra: Éves kriptovaluta-pénzmosás összegei (milliárd dollárban) 2019–2023 között
Forrás: a szerző szerkesztése Chainalysis 2024 alapján

Fontos megemlíteni továbbá, hogy a legnagyobb kriptovaluta-tőzsdék – köztük a Binance – már eltávolították platformjukról a monero és a zcash kereskedési lehetőségét, ami jól tükrözi a szabályozói nyomás erősödését.[25]

Csalások

A kriptovaluták gyors ütemű elterjedése és a köztudatba való beépülése jelentős hatást gyakorolt a digitális pénzügyi ökoszisztéma fejlődésére. A technológia újszerűsége, valamint a gyakran irreálisan magas hozamígéretek következtében mind több magánszemély és befektető dönt úgy, hogy befektet különféle kriptovalutákba. Ezzel párhuzamosan azonban az elmúlt években a csalások számának folyamatos emelkedése is megfigyelhető, ami a bűnözői körök gyors alkalmazkodását jelzi az új pénzügyi technológiákhoz. A kriptovalutákhoz kapcsolódó csalások számos formában

[23] A *know your customer* (KYC) elv olyan azonosítási és ellenőrzési folyamat, amelyet a pénzügyi szolgáltatók – például bankok, tőzsdék vagy kriptovaluta-platformok – kötelesek elvégezni annak érdekében, hogy azonosítsák ügyfeleiket (pl. személyazonosító okmány vagy lakcímigazolás alapján), valamint meggyőződjenek arról, hogy az ügyfél jövedelmei jogszerű forrásból származnak.
[24] European Union 2024b.
[25] CoinMarketCap 2024.

jelennek meg, amelyek közül az egyik leggyakoribb a magas hozamú befektetési csalások kategóriájába tartozó Ponzi-séma. Ez a megtévesztési forma arra épül, hogy az elkövetők az újonnan belépő befektetők által befizetett tőkéből fizetik ki a korábbi befektetőknek ígért hozamokat. A rendszer hosszú távon fenntarthatatlan, mivel mögötte nem húzódik meg valódi gazdasági tevékenység vagy jövedelemtermelő modell, csupán a folyamatos új befektetők bevonása biztosítja ideiglenes működését. Az új befektetőket gyakran manipulatív eszközökkel, például hamis hozamjelentésekkel, mesterségesen generált pozitív visszajelzésekkel és a már meglévő résztvevők ajánlásaival próbálják meggyőzni a csatlakozásról. Az ilyen típusú csalási technikák különösen ott bizonyulnak eredményesnek, ahol a kriptovaluták iránt érdeklődő, de pénzügyileg kevésbé tájékozott felhasználókat könnyen be lehet vonni a piacra, és ahol a szabályozási keretek hiányosak, illetve a jogérvényesítés nem működik kellő hatékonysággal.[26]

Az egyik legismertebb Ponzi-séma típusú csalási eset a Bitconnect platform 2018-as összeomlása volt. A szolgáltatás a felszínen legitim, felhasználóbarát kriptovalutaként és kereskedési felületként működött, ám valójában egy klasszikus Ponzi-sémát valósított meg, több ezer befektetővel. A rendszer működésének korai szakaszában akár évi 120%-os hozamot ígért a befektetőknek, amennyiben azok Bitconnect Coin (BCC) nevű tokenjeiket a platformon tárolták és ott kereskedtek velük. Ennek következtében a BCC-tranzakciók mintegy 95%-a házon belül zajlott, erősen korlátozva az átláthatóságot. További gyanúra adott okot, hogy a BCC kizárólag bitcoinért volt megvásárolható, fiat pénznemek használata nem volt lehetséges. Ez a működési modell nyilvánvalóan a nyomon követhetőség csökkentését szolgálta. A Bitconnect rendszeresen küldött hamisított kamatjelentéseket a befektetőknek, ám ezek a „hozamok" valójában az újonnan belépő felhasználók befizetéseiből származtak. 2018. január 17-én a BCC árfolyama drasztikusan összeomlott, és rövid időn belül 400 dollárról 27 dollárra zuhant. Ez a hirtelen árfolyamcsökkenés annak tudható be, hogy egyre több befektető ismerte fel a csalást, és megpróbálta minél gyorsabban kivenni a még elérhető tőkéjét a rendszerből. A befektetések teljes egészében kriptovalutában zajlottak, ami jelentős akadályt jelentett a bűnüldöző szervek számára a felelősök beazonosításában és az elkövetési lánc feltárásában. Bár néhány kulcsszereplőt sikerült azonosítani és bíróság elé állítani, több gyanúsított továbbra is ismeretlen vagy nem tudták előállítani őket, így a nyomozás máig sem zárult le teljes egészében.[27]

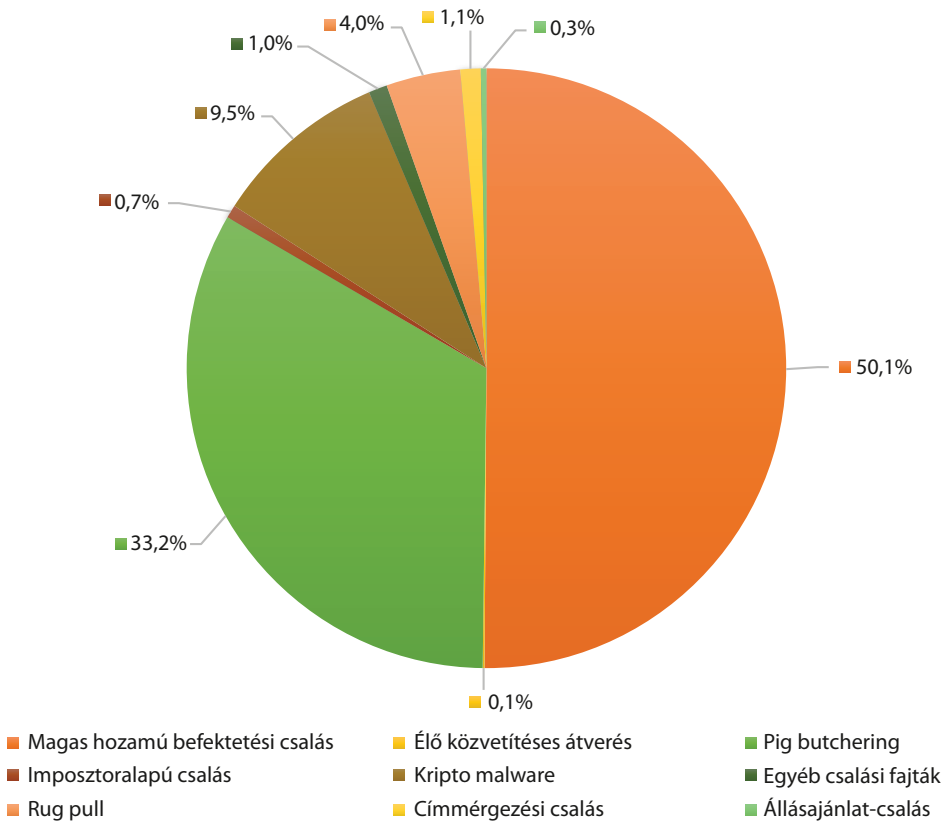
A Ponzi-séma mellett egy másik gyakran alkalmazott csalási forma a kriptovaluták esetén a pump and dump (P&D) metódus. A P&D ármanipulációs technika lényege, hogy egy fizetőeszköz árát mesterségesen felhajtják, mielőtt a korábban olcsón megvásárolt kriptovalutát magasabb áron értékesítik. Miután a kriptovalutát eladják, az árak drasztikusan visszaesnek, és a befektetők jelentős veszteségeket szenvednek el. A folyamat illusztrációja a 6. ábrán szerepel.

[26] Kerr et al. 2023.
[27] Baum 2018.

6. ábra: A pump and dump csalási módszer modellje
Forrás: a szerző szerkesztése Kamps–Kleinberg 2018 alapján

Több kutatás is rámutatott arra, hogy a P&D típusú ármanipulációk jellemzően szervezett módon valósulnak meg, úgynevezett P&D-csoportok létrejöttével. Ezek a közösségek kifejezetten azzal a céllal jönnek létre, hogy előre kiválasztott kriptovaluták árfolyamát mesterségesen felhajtsák, majd az így generált nyereséget realizálják. A csoportok elsősorban online platformokon – például Discordon vagy Telegramon – szerveződnek, ahol a manipulációt összehangoltan hajtják végre. Annak érdekében, hogy a lehető legnagyobb nyereséget érjék el, a rendelkezésre álló jelentések szerint ezek a csoportok szinte kizárólag alacsony piaci kapitalizációjú, kis forgalmú és kevésbé ismert kriptovalutákat céloznak. Az ilyen típusú eszközök árfolyama ugyanis sokkal érzékenyebb a hirtelen megnövekedett keresletre, ezáltal könnyebben manipulálható rövid időtávon belül.[28] A P&D-csalások egyik várható jövőbeli trendje a gyorsan változó globális témákhoz kapcsolódó, úgynevezett hype-tokenek létrehozása. Az elkövetők gyakran olyan új digitális tokeneket indítanak, amelyek aktuális társadalmi, politikai vagy kulturális jelenségekre építenek, így rövid idő alatt jelentős felhasználói érdeklődést generálnak. A kezdeti árfolyam-emelkedés után a szervezők hirtelen kivonják a befektetett tőkét, és a piac összeomlik. Egy szintén manapság elterjedt csalási módszer a pig butchering, amely a Chainalysis 2025-ös Crypto Crime Reportja szerint a második legtöbb bevételt hozó kriptocsalási forma. A módszer érzelmi manipuláción – leggyakrabban színlelt romantikus kapcsolaton – alapul, amely során a csalók hosszú bizalomépítés után veszik rá áldozatukat hamis kriptobefektetésekre. A jelentésben szereplő legelterjedtebb csalástípusok a 7. ábrán tekinthetők meg. A megoszlásból kitűnik, hogy a klasszikus pénzügyi átverések (például befektetési csalások és pig butchering) dominálnak, míg a kifinomult technológiai jellegű csalások kisebb, de nem elhanyagolható szeletet képviselnek. Ez a tendencia arra utal, hogy a kriptovaluta-alapú csalások sikerességében a pszichológiai manipuláció továbbra is nagyobb szerepet játszik, mint a tisztán technikai eszközök.[29]

[28] Kamps–Kleinberg 2018.
[29] Chainalysis 2025.



7. ábra: Kriptovaluta-alapú csalásokból szerzett bevételek altípusok szerint
Forrás: a szerző szerkesztése Chainalysis 2025 alapján

Zsarolóvírusok, váltságdíjfizetések kriptovalutában

A zsarolóvírusos támadások az elmúlt évek egyik legtöbbet elkövetett és legsúlyosabb következményekkel járó kiberbűnözési formájává váltak. Ezek a rosszindulatú programok a megfertőzött eszközökön tárolt adatokat titkosítják, és azok visszafejtéséért váltságdíjat követelnek az áldozattól. A váltságdíjakat jellemzően kriptovalutákban határozzák meg, ami nagymértékben hozzájárul a támadók anonimitásának fenntartásához.

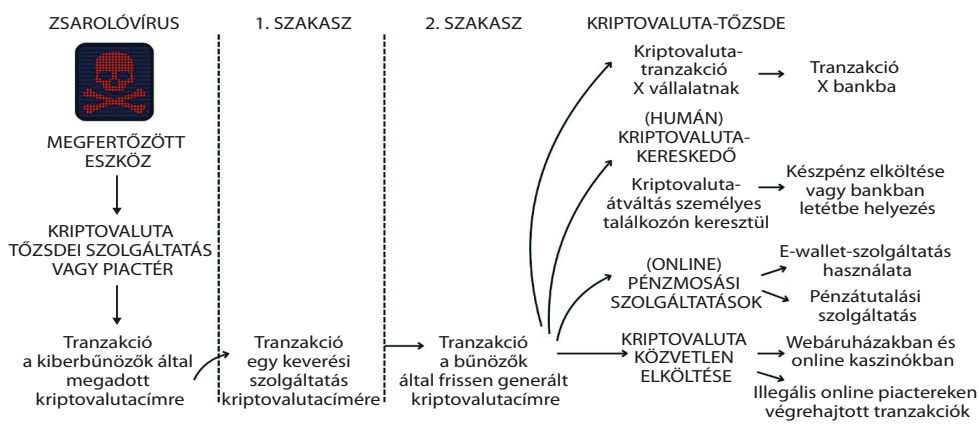
A Chainalysis 2025-ös jelentése szerint 2024-ben a zsarolóvírus-támadásokhoz köthető váltságdíj-kifizetések összege 2%-kal emelkedett az előző évhez képest, és elérte a 459,8 millió dollárt, szemben a 2023-as 449,1 millió dolláros adattal.[30] A növekedés hátterében több tényező áll, amelyek közül kiemelkedik a zsarolóvírus

[30] Chainalysis 2024.

mint szolgáltatás[31] (RaaS-) modell térnyerése. Ez a szolgáltatásalapú megközelítés lehetővé teszi, hogy technikai háttérrel kevésbé rendelkező elkövetők is hozzáférjenek professzionálisan fejlesztett zsarolóvírusokhoz, ezzel jelentősen növelve a támadások számát és hatékonyságát. A TRM Labs 2025-ös jelentése szerint a RaaS-modell térnyerésével párhuzamosan 2024-ben több új zsarolóvírus-csoport is megjelent, például a Brain Cipher, dAn0n, DragonForce, Fog, Funksec, RansomHub, Sarcoma és Trinity, ami jelzi a piaci szereplők folyamatos bővülését és a támadások diverzifikálódását.[32]

A kriptovaluták részleges anonimitást biztosító jellege szintén elősegíti a zsarolóvírus-támadások sikerét, mivel lehetővé teszi, hogy az elkövetők személyazonosságuk felfedése nélkül követeljenek és fogadjanak el váltságdíjat. A támadók anonimitását nem kizárólag a kriptovaluták technikai sajátosságai biztosítják, hanem gyakran további eszközöket is igénybe vesznek, mint például coin mixereket vagy a dark weben működő escrow szolgáltatásokat, amelyek még inkább megnehezítik az azonosítást és a tranzakciók visszakövetését. A váltságdíjak kifizetésére továbbra is a bitcoin a leggyakrabban használt kriptovaluta, mivel széles körben hozzáférhető és a legtöbb szereplő által elfogadott fizetőeszköz a kiberbűnözői ökoszisztémában. Ugyanakkor megfigyelhető, hogy a monero egyre népszerűbbé válik az elkövetők körében, mivel jelentősen magasabb szintű tranzakciós anonimitást kínál a bitcoinhoz képest.[33]

Hazai eset a 2021 márciusában bekövetkezett zsarolóvírus-támadás, amely az UNIX Autó Kft.-t érte, és ahol a váltságdíjat moneróban követelték.[34] Egy másik jelentős eset 2021 áprilisában történt, amikor a Colonial Pipeline, az USA legnagyobb üzemanyagvezeték-hálózatának üzemeltetője, zsarolóvírus-támadás áldozatává vált. A támadók, a DarkSide nevű kiberbűnöző csoport, 75 bitcoin (akkoriban körülbelül 4,4 millió USD értékben) váltságdíjat követeltek és szereztek meg[35] (8. ábra).



8. ábra: A zsarolóvírusokból származó nyereség pénzmosási modellje
Forrás: a szerző szerkesztése Custers–Oerlemans–Pool 2020 alapján

[31] Illegális üzleti modell, amelyben a zsarolóvírusok készítői szoftverként kínálják fel a kártékony programokat más bűnözőknek, akik így technikai tudás nélkül is képesek zsarolóvírus-támadásokat végrehajtani. A támadók általában megosztják a befolyt váltságdíjat a RaaS-szolgáltatóval, aki cserébe technikai támogatást, frissítéseket és infrastruktúrát biztosít.
[32] TRM Labs 2025.
[33] Custers–Oerlemans–Pool 2020.
[34] UNIX Autó Kft. 2024.
[35] Beerman et al. 2023.

A *The Evolution of Cryptocurrency and Cyber Attacks* című tanulmány, azt vizsgálta, hogy van-e kimutatható összefüggés a zsarolóvírusok terjedése és a kriptovaluták egyre szélesebb körű használata között. A kutatás egyik központi kérdése az volt, hogy a zsarolóvírusok kialakulása és fennmaradása független lehet-e a kriptovalutáktól, vagy pedig ezek kulcsszerepet játszanak a kibertámadások ezen formájának terjedésében. Az eredmények arra mutattak, hogy nem feltételezhető közvetlen korreláció a két jelenség között, és a zsarolóvírusok kriptovaluta nélkül is létezhetnek. Ezt támasztja alá az a tény is, hogy zsarolóvírusok már jóval a kriptovaluták megjelenése előtt, például a bitcoin elterjedését megelőzően is jelen voltak. Ennek egyik legkorábbi példája az AIDS Trojan (vagy más néven PC Cyborg), amely 1989-ben jelent meg, amikor is egy konferencián húszezer résztvevőnek osztották szét floppylemezeken. A megfertőzött számítógépek felhasználóitól 189 dollárt követeltek.[36]

Bár a kutatás nem talált egyértelmű korrelációt a kriptovaluták és a zsarolóvírusok elterjedése között, manapság a zsarolóvírusok túlnyomó többsége mégis kriptovalutában követeli a váltságdíjat. Ez azt sugallja, hogy a kriptovaluták anonimitása és nehezebb nyomon követhetősége olyan tényezők, amelyek hozzájárulhatnak e bűncselekmények fennmaradásához és terjedéséhez, mivel megkönnyítik a támadók számára az illegális pénzügyi tranzakciókat.

Terrorizmus finanszírozása kriptovalutákon keresztül

A terrorizmus finanszírozása azon folyamatokat foglalja magában, amelyek során terrorista szervezetek pénzügyi forrásokat szereznek és használnak fel tevékenységeik előkészítésére, megszervezésére és végrehajtására. A pénzügyi támogatás nemcsak konkrét terrortámadások megvalósításához szükséges, hanem a szervezetek mindennapi működésének fenntartásához is, beleértve a toborzást, a kiképzést, a fegyverbeszerzést, a logisztikai háttér biztosítását, valamint a tagok és hozzátartozóik anyagi támogatását.[37] Bár egy-egy támadás viszonylag alacsony költségű lehet, a terrorszervezetek működtetése jelentős anyagi forrásokat igényel. A szigorodó pénzügyi ellenőrzések miatt ezek a csoportok egyre gyakrabban fordulnak alternatív eszközökhöz, mint például a kriptovalutákhoz. Egy sikeres terrorszervezet – hasonlóan a bűnözői csoportokhoz – olyan, amely képes hatékony pénzügyi infrastruktúrát kiépíteni és fenntartani. Ennek érdekében a csoportnak különféle finanszírozási forrásokat kell kialakítania, valamint olyan eszközöket kell fejlesztenie, amelyek megnehezítik a források és a finanszírozott tevékenységek közötti kapcsolatok felderítését. A kriptovaluták vonzó megoldásnak tekinthetők a terrorizmus finanszírozására, mivel olyan jellemzőkkel rendelkeznek, mint a letagadhatatlanság, a központi felügyelet hiánya, az alacsony használati költség, a viszonylag egyszerű használat, valamint a helyszín és a valuta változtathatóságának rugalmassága, a tranzakciók feldolgozási sebessége, a működés bonyolultsága és a globális elérhetőség, illetve a már említett anonimitást elősegítő módszerek. A dark web felületet biztosít a terrorszervezetek számára, hogy kriptovalutában adományokat gyűjtsenek céljaik finanszírozására, amely

[36] Berry 2022.
[37] Alfieri 2022.

összegeket később fegyverek és robbanóanyagok beszerzésére fordíthatnak különböző, szintén dark webes piactereken keresztül. Példaként említhető a „Támogasd az Iszlám Harcot nyom nélkül" nevezetű dark webes oldal (9. ábra), amely bitcointranzakciók útján gyűjt adományokat egy adott Bitcoin-címre a dzsihád támogatására. A felületen emellett egy PDF-fájl is elérhető, amely útmutatóként szolgál az anonim pénzátutalások végrehajtásához.[38]

A Chainalysis megállapítása alapján a Hamasz Izz ad-Din al-Kasszám Brigádja (AQB) „az egyik legnagyobb és legkifinomultabb kriptovaluta-alapú terrorizmusfinanszírozási kampányt valósította meg, amit valaha tapasztaltak". 2019-ben az AQB megpróbált bitcoint használva adományokat gyűjteni támogatóitól, és módszereit folyamatosan finomította, ahogy a bűnüldöző szervek akadályozni próbálták erőfeszítéseit. A csoport egy QR-kódot helyezett el a weboldalán, amely egy Bitcoin-címhez irányította az adományozókat. Nem sokkal később azonban a hatóságok befagyasztották a számlát, és megvizsgálták annak tulajdonosát és tranzakcióit. Az AQB erre reagálva lecserélte a QR-kódos Bitcoin-címet egy privát tárcához tartozó új címre. Bár az AQB úgy gondolta, hogy ez a privát tárca növeli az anonimitást, a bűnüldöző szervek elemzői képesek voltak nyomon követni a csoport tárcatranzakcióit és adományait. A tárcát végül leállították. Az AQB ismét változtatott a bitcoinadományok gyűjtésének módszerén. Ezúttal a weboldal minden egyes adományozó számára külön-külön Bitcoin-címet generált, amelyre a támogatók pénzt küldhettek. A weboldal egy oktatóvideót is tartalmazott, amely részletesen bemutatta, hogyan lehet a legnagyobb anonimitás mellett adományozni. A videó két adományozási lehetőséget ajánlott: a hawalát[39] vagy egy privát Bitcoin-tárca használatát. A hawala egy informális pénzátutalási rendszer, amely a bizalmon alapul. Ha ezt a módszert választották, az adományozók megadhatták a Bitcoin-címet, valamint az adomány összegét fiat pénzben, amit a hawala szolgáltató bitcoinban utalt tovább a megadott címre. Az útmutató emellett azt is elmagyarázta, hogyan lehet privát Bitcoin-tárcát létrehozni, és egy ajánlott kriptotőzsdén keresztül bitcoint vásárolni, majd azt átutalni a megfelelő címre. Ez a kifinomult rendszer egyre nehezebbé tette a pénzügyi tranzakciók nyomon követését. Az AQB több mint 10 000 dollárnyi adományt gyűjtött össze, amíg az amerikai hatóságok 2020-ban le nem foglalták az adománygyűjtő oldalt. Ez az eset is rávilágít arra, hogy az AQB nemcsak sikeresen használta ki a kriptovalutát, hanem folyamatosan alkalmazkodott is, amikor a bűnüldöző szervek akadályozták tevékenységét.[40]

A kriptovaluták felhasználása a dark web piacokon

A dark webes piacterek által nyújtott technológiai anonimitás kiemelkedően kedvező feltételeket teremt az illegális tevékenységek lebonyolításához. Ezeken a platformokon széles skálán mozognak az elérhető illegális termékek és szolgáltatások – például

[38] Majumder–Routh–Singha 2019.

[39] A *hawala* egy alternatív pénzátutalási rendszer, amelyben a pénz fizikailag nem hagyja el a küldő országot, mégis eljut a címzetthez. A folyamat alapját két egymással kapcsolatban álló és egymásban megbízó közvetítő – úgynevezett hawalaügynökök – közti informális megállapodás képezi. Ők egyeztetik egymással a szükséges összeget, amelyet banki vagy hivatalos pénzügyi csatornák igénybevétele nélkül adnak át.

[40] Alfieri 2022.

kábítószerek, fegyverek, hamis iratok vagy kiberbűnözési eszközök –, amelyek folyamatosan változó kínálata dinamikus és nehezen kontrollálható környezetet hoz létre. A kriptovaluták, különösen a bitcoin és a privacy coinok, jelentős szerepet játszanak e piacterek működésében, mivel decentralizált és részben vagy teljesen anonimizált fizetési lehetőséget biztosítanak. Ezáltal a felhasználók úgy tudják lebonyolítani tranzakcióikat, hogy személyazonosságuk rejtve maradjon. A The Onion Router (TOR) hálózat technikai infrastruktúrája tovább fokozza a résztvevők anonimitását. A TOR úgynevezett réteges titkosítási technológiát alkalmaz, amely lehetővé teszi, hogy a felhasználók internetes forgalma többlépcsős csatornákon keresztül, véletlenszerűen kiválasztott csomópontokon haladjon át. Ennek köszönhetően a felhasználók tevékenységei és IP-címeik rejtve maradnak, így mind a piacterek üzemeltetői, mind pedig a vásárlók számára fokozott védelmet nyújt a digitális nyomon követhetőséggel szemben.[41]

9. ábra: Dzsihadista és terrorista szervezetek támogatására irányuló adománygyűjtő kampányt hirdető weboldalak

Megjegyzés: A weboldal az adományozást moneróban bonyolítja.

Forrás: TRM Labs 2025

A Chainalysis 2024-es Crypto Crime Reportja szerint a dark web piacterek 2023-ban 1,7 milliárd dollárnyi bevételt generáltak, amely jelentős növekedést jelent a megelőző év adataihoz képest. A bővülés hátterében részben a Hydra Market 2022-es bezárása állt, amely alapvetően alakította át a dark web illegális kereskedelmi ökoszisztémáját.

[41] Kavallieros et al. 2021.

A Hydra korábbi dominanciája miatt annak megszűnése nem visszaesést, hanem szerkezeti átrendeződést eredményezett: új szereplők léptek a piacra, és a Hydra egykori felhasználói más platformokra migráltak. A jelentés adatai alapján a dark web piacterek nem gyengültek, csupán átszerveződtek, ami teret nyitott új szolgáltatóknak és üzleti modelleknek.[42]

A 2025-ben publikált *Crypto Crime Report* szerint bár a kriptovaluta-alapú bűncselekmények volumene történelmi csúcsot ért el, a dark web piacterek és a személyazonosság-lopással kapcsolatos szolgáltatások bitcoinalapú bevételei csökkentek. 2024-ben a dark web piacterek bevétele több mint 2 milliárd, ami jelentős visszaesés az előző évekhez képest. A Hydra Market megszűnését követően új szereplők vették át a vezető pozíciót, közülük a Kraken piactér emelkedett ki, amely 737 millió dollár értékű bitcoinforgalmat bonyolított le, így vált piacvezetővé. A jelentés azt is megállapítja, hogy a Bitcoin transzparenciája miatt egyre több szereplő tér át a monero használatára.[43]

A kriptovaluták használata mellett a dark web piacterein a tranzakciók biztonságát és titkosságát gyakran escrow (letéti) mechanizmusok alkalmazásával biztosítják. Az escrow rendszer lényege, hogy egy harmadik fél ideiglenesen tárolja a kriptovalutát, amíg az eladó teljesíti az ígért szolgáltatást, ezáltal csökkentve a csalások kockázatát. A hagyományos dark webes piacokon a vásárlók összegeit először levonják a digitális pénztárcából, majd egy escrow számlára helyezik, amelyet a piactér vagy egy harmadik fél kezel. Ez a folyamat biztosítja, hogy a pénz csak a vásárlás véglegesítésekor kerüljön át az eladóhoz. Az escrow rendszerek azonban nem teljesen kockázatmentesek. A pénzt kezelő harmadik fél visszaélhet a felhasználók bizalmával, például „kilépési csalás" (exit scam[44]) formájában, amikor a szolgáltató váratlanul eltűnik a letéti pénzekkel. Egy figyelemreméltó eset 2015 márciusában történt, amikor az Evolution dark web piactér hirtelen bezárta kapuit, és az üzemeltetők több mint 11 millió euró értékű kriptovalutával tűntek el. Ez az eset kiemeli a bizalom fontosságát az escrow rendszerek működésében.[45]

Nemcsak a kilépési csalások, hanem a hatósági rajtaütések is jelentős kockázatot jelentenek a dark webes piacokon. Például 2024 októberében a hatóságok felszámolták a világ legnagyobb dark web piacát, amely a Bohemia és a Cannabia platformokból állt. A művelet során több mint 6,5 millió font értékű kriptovalutát foglaltak le, és letartóztatták a két adminisztrátort. A hatósági rajtaütések és a kilépési csalások egyaránt rávilágítanak arra, hogy az escrow rendszerek használatával a felhasználók gyakran kiszolgáltatottá válnak olyan tényezőknek, amelyek felett nincs kontrolljuk.[46]

[42] Chainalysis 2024.
[43] Chainalysis 2025.
[44] Az *exit scam* (kilépési csalás) olyan szándékos és előre megtervezett csalási forma, amely során egy – kezdetben megbízhatónak vagy legitimnek tűnő – szolgáltató (pl. kriptovaluta-tőzsde, befektetési platform vagy *dark net* piactér) hirtelen leállítja működését, és az ügyfelek letéti összegeit eltulajdonítja. A csalás a felhasználók bizalmára és a platform korábbi jó hírnevére épít, amelyet a későbbi tőkekiáramlás maximalizálása érdekében tudatosan építenek fel.
[45] Intel 471 2021.
[46] Lakshmanan 2024.

Diszkusszió

A kutatás eredményei alátámasztják azt a feltételezést, hogy a kriptovaluták technológiai sajátosságai, különösen az anonimitás kiemelt szerepet játszanak a kiberbűnözés új formáinak kialakulásában és terjedésében. A Chainalysis 2024-es és 2025-ös jelentési adatai alapján kirajzolódik, hogy bár a bitcoin továbbra is dominál az illegális tranzakciók során, de az újabb típusú kriptovaluták, mint a stablecoinok vagy az ethereum gyors térnyerése új kihívásokat jelent a nyomozó hatóságok számára. Ezzel párhuzamosan megállapítható, hogy a privacy coinok marginális piaci súlyuk ellenére kiemelt szerepet töltenek be a pénzmosásban, a zsarolóvírusos támadások lebonyolításában, valamint a dark webes piactereken végbemenő tranzakciók anonimizálásában.

A coin mixer szolgáltatások elemzése megerősítette azt a hipotézist, miszerint a bűnelkövetők tudatosan alkalmaznak olyan technológiai megoldásokat, amelyek jelentősen rontják a visszafejthetőség esélyét. A Monero esete különösen jól példázza, hogy a natív anonimizálási mechanizmusok mennyiben képesek kiváltani a hagyományos coin mixerek funkcióit, sőt meghaladni azok hatékonyságát. A kutatás során feltárt esettanulmányok szemléletesen mutatják be, hogy a kriptovaluták alkalmazása messze túlmutat a puszta pénzmozgatáson. A kriptovaluta a kiberbűnözés eszközévé válik, amely egyszerre szolgál tranzakciós infrastruktúraként, álcázási technikaként és pénzügyi motivációs közegként.

Ezen eredmények tükrében a kutatás két tézise fogalmazható meg:

T1: A Chainalysis 2024-es és 2025-ös jelentései alapján az elmúlt években markáns eltolódás figyelhető meg a bűnözők által használt kriptovaluták körében. Míg korábban a bitcoin dominanciája volt egyértelmű az illegális tranzakciókban, 2024-re a stablecoinok vették át a vezető szerepet, amint az a 3. ábrán is látható. Ugyanakkor – ahogy azt az ábra magyarázatánál az alapfogalmak fejezetben kifejtettük – a stablecoinok több tokenből álló kategóriát alkotnak, ezért továbbra is megalapozottan kijelenthető és alátámasztható a hipotézis, miszerint a bitcoin még mindig a vezető kriptovaluta az illegális tevékenységekben. A stablecoinok és az ethereum szerepe azonban folyamatosan növekszik, elsősorban a DeFi-ökoszisztéma, az okosszerződések és a széles körű piaci integráció következtében. A privacy coinok globálisan marginális volumennel rendelkeznek, ugyanakkor bizonyos bűncselekménytípusokban – különösen a zsarolóvírusos váltságdíjak kifizetésében és a dark webes tranzakciókban – felülreprezentáltak. A szigorodó szabályozások, például az EU 2024/1624 AMLR rendelete és a nagy kriptotőzsdék privacy coin kivezetései paradox módon tovább növelik az anonim platformok iránti keresletet az illegális piacon. Emellett egyre elterjedtebbek a bűnelkövetők körében a többlépcsős tranzakciós minták, amelyek során különböző kriptovaluták között váltanak – például a bitcoinból ethereumra, majd moneróra – kifejezetten a tranzakciók nyomon követhetőségének csökkentése érdekében. Ez a gyakorlat a nyomozó hatóságok számára összetett technológiai és jogi kihívásokat eredményez. A jövőbeni empirikus és kvantitatív elemzések során indokolt lehet részletesen vizsgálni, hogy a stablecoinok egyes tokenjein belül melyek mutatnak kiemelkedő illegális forgalmi aktivitást.

T2: A kriptovaluta-tranzakciók visszakövethetőségét akadályozó technológiák (például coin mixerek, privacy coinok, escrow rendszerek) nem csupán elméleti lehetőségek,

hanem a kiberbűnözésben széles körben alkalmazott eszközök. Ez a gyakorlat közvetlenül alátámasztja a második hipotézist, miszerint a bűnelkövetők folyamatosan alkalmazzák az anonimizálást és a blokkláncon való visszakövethetőség akadályozását szolgáló technológiákat, ami állandó kihívást jelent a bűnüldöző szervek számára. A macska-egér játék logikája egyértelműen megfigyelhető: a technológiai fejlődés mindkét felet egyre kifinomultabb, fejlettebb és innovatívabb módszerek bevetésére ösztönzi, így a nyomozások folyamatosan új akadályokba ütköznek. A kutatás azt is feltárta, hogy a coin mixerek és privacy coinok használata már nem kizárólag a technikailag felkészült bűnelkövetők kiváltsága, hanem felhasználóbarát formában szélesebb kör számára is hozzáférhetővé vált. Ezzel párhuzamosan a bűnüldöző hatóságok a nemzetközi együttműködések erősítésével, valamint a transzparenciát növelő szabályozási keretek, például az FATF Travel Rule és a MiCA alkalmazásával igyekeznek ellensúlyozni ezt a tendenciát.

A fentiek alapján összegzésként kijelenthető, hogy a kriptovaluták jogi, technológiai és bűnüldözési szempontból is egy olyan hibrid kihívást képeznek, amely nem kezelhető pusztán szabályozói, informatikai vagy rendészeti válaszokkal. A hatékony fellépéshez szükség van multidiszciplináris megközelítésre, amely ötvözi a bűnügyi pénzügyi elemzést, a blokkláncelemzést, a nemzetközi együttműködést és a szabályozói eszköztár folyamatos frissítését.

A cikksorozat második része azon technikai és nyomozati módszerek bemutatására fókuszál, amelyek révén a rendvédelmi szervek képesek fellépni a kriptovalutákhoz köthető bűncselekményekkel szemben. Bemutatjuk azokat az eszközöket és eljárásokat, amelyek révén lehetővé válik a kriptovalutákkal összefüggő jogsértések felderítése, a tranzakciók visszakövetése, valamint a digitális bizonyítékok büntetőeljárásban való felhasználása, ezáltal gyakorlati válaszokat adva a jelen tanulmányban feltárt elméleti kihívásokra.

Felhasznált irodalom

Albrecht, Chad et al. (2019): The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control,* 22(2), 210–216. Online: https://doi.org/10.1108/JMLC-12-2017-0074

Alfieri, Carolyn (2022): Cryptocurrency and National Security. *International Journal on Criminology,* 9(1), 21–48. Online: https://doi.org/10.18278/ijc.9.1.3

Baum, Stafford C. (2018): *Cryptocurrency Fraud: A Look Into the Frontier of Fraud.* Honors College Theses, 2018. november 19. Online: https://digitalcommons.georgiasouthern.edu/honors-theses/375

Beerman, Jack et al. (2023): A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW),* 8–15. Online: https://doi.org/10.1109/CCGridW59191.2023.00017

Berry, Hala Strohmier (2022): The Evolution of Cryptocurrency and Cyber Attacks. *2022 International Conference on Computer and Applications (ICCA),* 1–7. Online: https://doi.org/10.1109/ICCA56443.2022.10039632
Chainalysis (2024): *The 2024 Crypto Crime Report.* Online: https://go.chainalysis.com/crypto-crime-2024.html
Chainalysis (2025): *The 2025 Crypto Crime Report.* Online: https://go.chainalysis.com/2025-Crypto-Crime-Report.html
CoinMarketCap (2024): *Binance Delists Privacy-Focused Cryptocurrencies in Multiple European Countries.* Online: https://coinmarketcap.com/academy/article/binance-delists-privacy-focused-cryptocurrencies-in-multiple-european-countries
Custers, Bart – Oerlemans, Jan-Jaap – Pool, Ronald (2020): Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice,* 28, 121–152. Online: https://doi.org/10.1163/15718174-02802002
Europol (2015): Darknets–IOCTA 2015. Online: www.europol.europa.eu/iocta/2015/darknets.html
FATF (2021): *12 Month Review of the Revised FATF Standards. Virtual Assets and VASPs.* Online: www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html
Intel 471 (2021): *How Cryptomixers Allow Cybercriminals to Clean Their Ransoms.* Online: https://intel471.com/blog/cryptomixers-ransomware
Kamps, Josh – Kleinberg, Bennett (2018): To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps. *Crime Science,* 7, 18. Online: https://doi.org/10.1186/s40163-018-0093-5
Kavallieros, Dimitrios et al. (2021): Understanding the Dark Web. In Akhgar, Babak et al. (szerk.): *Dark Web Investigation. Security Informatics and Law Enforcement.* Cham: Springer, 3–26. Online: https://doi.org/10.1007/978-3-030-55343-2_1
Kerr, David S. et al. (2023): Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks,* 11(3). Online: https://doi.org/10.3390/risks11030051
Lakshmanan, Ravie (2024): Bohemia and Cannabia Dark Web Markets Taken Down After Joint Police Operation.*The Hacker News,* 2024. október 11. Online: https://thehackernews.com/2024/10/bohemia-and-cannabia-dark-web-markets.html
Levi, Michael (2002): Money Laundering and Its Regulation. *The ANNALS of the American Academy of Political and Social Science,* 582(1), 181–194. Online: https://doi.org/10.1177/000271620258200113
Li, Yannan et al. (2021): Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. *IEEE Transactions on Dependable and Secure Computing,* 18(2), 679–691. Online: https://doi.org/10.1109/TDSC.2019.2910058
Majumder, Amit – Routh, Megnath – Singha, Dipayan (2019): A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing. In Das, Ramesh Chandra (szerk.): *The Impact of Global Terrorism on Economic and Political Development.* Emerald Publishing Limited, 125–138. Online: https://doi.org/10.1108/978-1-78769-919-920191012

Mariani, Juraj – Homoliak, Ivan (2025): SoK: A Survey of Mixing Techniques and Mixers for Cryptocurrencies. *arXiv,* 2025. április 28. Online: https://doi.org/10.48550/arXiv.2504.20296
Monero (2024): *Moneropedia: Ring Signature.* Online: www.getmonero.org/resources/moneropedia/ringsignatures.html
Mukhopadhyay, Ujan et al. (2016): A Brief Survey of Cryptocurrency Systems. *2016 14th Annual Conference on Privacy, Security and Trust (PST),* 745–752. Online: https://doi.org/10.1109/PST.2016.7906988
Nakamoto, Satoshi (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System.* Online: www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System
Noether, Shen (2015): *Ring Signature Confidential Transactions for Monero.* Cryptology ePrint Archive. Online: https://eprint.iacr.org/2015/1098
Schneider, Friedrich – Windischbauer, Ursula (2008): Money Laundering: Some Facts. *European Journal of Law and Economics,* 26(3), 387–404. Online: https://doi.org/10.1007/s10657-008-9070-x
Southern District of New York (2025): *Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty.* United States Department of Justice, 2025. augusztus 6. Online: www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-plead-guilty
Tekiner, Ege et al. (2021): SoK: Cryptojacking Malware. *2021 IEEE European Symposium on Security and Privacy (EuroS&P),* 120–139. Online: https://doi.org/10.1109/EuroSP51992.2021.00019
TRM Labs (2025): *2025 Crypto Crime Report.* Online: www.trmlabs.com/resources/reports/2025-crypto-crime-report
UNIX Autó Kft. (2024): Hackertámadás – 2021. 03. 30. Online: www.unixauto.hu/hirlevel/hackertamadas
Zhang, Zongyang et al. (2020): A Refined Analysis of Zcash Anonymity. *IEEE Access,* 8, 31845–31853. Online: https://doi.org/10.1109/ACCESS.2020.2973291

Jogi források

Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete (2023. május 31.) a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról
Az Európai Parlament és a Tanács (EU) 2024/1624 rendelete (2024. május 31.) a pénzügyi rendszer pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről
Az Európai Parlament és a Tanács (EU) 2024/1640 irányelve (2024. május 31.) a pénzügyi rendszer pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzése érdekében a tagállamok által létrehozandó mechanizmusokról, az (EU) 2019/1937 irányelv módosításáról, és az (EU) 2015/849 irányelv módosításáról és hatályon kívül helyezéséről