



37. Országos Tudományos Diákköri Konferencia

Állam- és Jogtudományi Szekció

Budapest, 2025. március 24–26.

Rendező intézmény:

Károli Gáspár Református Egyetem

Állam- és Jogtudományi Kar



Állam- és Jog-
tudományi Szekció

**A digitális bizonyítékok jelentősége a
büntetőeljárásban, különös tekintettel a
kriptoalutával elkövetett bűncselekményekre**

Kézirat lezárásnak dátuma:

2024. 12. 10.

NYILATKOZAT A MESTERSÉGES INTELLIGENCIA (MI) HASZNÁLATÁRÓL

A DOLGOZAT SZERZŐJEKÉNT NYILATKOZOM, HOGY A DOLGOZAT ELKÉSZÍTÉSE SORÁN ÉRDEMBELI SEGÍTSÉGET **NEM** NYÚJTOTT SZÁMOMRA A MESTERSÉGES INTELLIGENCIA ÉS KIZÁRÓLAGOSAN SAJÁT SZELLEMI ALKOTÁSOMAT JELENÍTEM MEG E DOLGOZATBAN.

TARTALOMJEGYZÉK

I.	Bevezetés.....	3
II.	Kutatásmódszertan	4
III.	Alapfogalmak és elméleti háttér.....	6
	1. A kiberbűncselekmény (cybercrime) fogalmi értelmezése	6
	2. A kriptovaluták kialakulásának rövid története, működése.....	7
	3. A kriptovaluták fogalmi köre	10
IV.	Kriptovalutákkal leggyakrabban elkövetett bűncselekmények az Európai Unióban....	12
V.	Kriptovalutákkal leggyakrabban elkövetett bűncselekmények az USA-ban	14
VI.	A hagyományos bizonyításelmélet.....	16
VII.	Az elektronikus bizonyíték fogalmi meghatározásának fejlődése	17
IX.	A blokklánc technológia hogyan használható fel a bizonyításban?	20
	1. A CoC, azaz a felügyeleti lánc – mint bizonyítási eszköz – bemutatása a Bitcoin tekintetében.....	22
	2. A felügyeleti lánc fő követelményei, ahhoz, hogy a bizonyításban felhasználható legyen.....	23
X.	A lefoglalás bemutatása az elektronikus adat esetén, különös tekintettel a Bitcoin kriptovalutára, avagy „Őrizd meg mindent, ne változtass semmin!”	25
	A bizonyítás nehézségei	27
XI.	Uniós szintű jogforrások	29
	1. Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.....	29
	2. Az Európai Parlament és a Tanács (EU) 2023/1543. rendelete	29
	3. A NIS és a NIS 2 IRÁNYELV	30
	A SIRIUS projekt.....	31
XII.	Nemzetközi kitekintés, avagy az Amerikai Egyesült Államok szabályozása, különös tekintettel Florida Állam szabályozására	32
	Florida State v. Espinoza eset bemutatása.....	33
	Elemzés.....	36
XIII.	Javaslat	37
XIV.	Záró gondolatok	38
	FORRÁS- ÉS IRODALOMJEGYZÉK	39
	TÁBLÁZAT, VALAMINT ÁBRAJEGYZÉK	47

I. Bevezetés

A digitális technológia fejlődése megváltoztatta az élet minden területét, így a bűnözést és a bűnüldözést is. Napjainkban a bűnelkövetők egyre gyakrabban hagyatkoznak az online tér adta lehetőségekre. Ez kihatással van a nyomozó hatóságokra is, hiszen lépést kell tartaniuk az új technikai vívmányokkal. Az egyik legnagyobb kihívás a digitális bizonyítékok begyűjtése, értékelése, kezelése és jogszerű felhasználása. A kriptovaluták megjelenése új dimenziót teremtett a pénzügyi tranzakciók világában, ugyanakkor új lehetőségeket kínál a bűnözők számára is.

A digitális bizonyítékok szerepe nemcsak ezeknek a bűncselekményeknek a felderítésében, hanem a bírósági eljárásokban is rendkívül szignifikánsak. A kriptovaluták tranzakcióinak nyomon követése, és ezek tárolására hivatott tárcák beazonosítása olyan különleges szakértelmet és technológiai infrastruktúrát igényel, amelyek szükségesek a hatékony nyomozás és az igazságszolgáltatás érdekében.

A tanulmány áttekinti a digitális bizonyítékok kezelésének kereteit, valamint a felügyeleti lánc felhasználását, mint bizonyítási eszközt. Ismerteti a lefoglalást, mint kényszerintézkedést, különös tekintettel a Bitcoin kriptovalutára, hiszen a lefoglalás a bizonyítékok biztosításának primer módja, s a bizonyíték hiányában – vagy sérült bizonyíték esetén – az elkövetők büntetőjogi felelősségre vonása nem lenne megvalósítható a büntetőeljárás során.

E fajta elektronikus adatok feltárása nem olyan egyszerű, mint azt elsőre gondolnánk. Rengeteg új készség, technika és együttműködés szükséges a szakértők részéről is az eredményesebb nyomozás, valamint a bizonyítás sikerességének érdekében.

A téma relevanciáját az indokolja, hogy egyre több olyan deliktum valósul meg, amelyekben a digitális bizonyítékok nélkülözhetetlenek a büntetőjogi felelősség megállapításához.

A felmerült gondolataim alapján munkám során a következő hipotéziseket állítottam fel:

- 1. A kriptovalutával elkövetett bűncselekmények száma növekvő tendenciát mutat, mind európai, mind amerikai szinten.*
- 2. Feltételezem, hogy a bizonyítás a kriptovalutával elkövetett bűncselekmények esetén komplikáltabb lehet, olyan bűncselekmény bizonyításához képest, amelynél a bizonyítékok kézzelfoghatók.*

II. Kutatásmódszertan

A dolgozathoz szükséges kutatás módszertana elsősorban primer és szekunder forráselemzés volt. Primer források volt többek közt a jogszabályok, rendeletek, törvények, kerethatározatok. Szekunder források voltak a témáról korábban írt elemzések. Dolgozatomra jellemző, hogy a kutatás több szakaszában külföldi szakirodalmat részesítettem több szakaszában is előnyben. Ennek oka az, hogy a hazai szakirodalom az általam választott témával még nem foglalkozott olyan mértékben, mint a külföldi. Dolgozatom e tekintetben hiánypótló mű.

Több fogalmat vizsgáltam, különös tekintettel a „*cybercrime*”-ra, az elektronikus adatra, valamint a digitális bizonyítékok meghatározására. Történeti áttekintéssel vezettem le, hogy a fogalmak a kor kihívásaihoz képest hogyan fejlődtek, s alakultak át. A „*cybercrime*” tekintetében megállapítható volt, hogy sem a hazai, sem a külföldi szakirodalom nem állapodott meg egy egységes fogalom meghatározásban. Ennek következtében az általam felkeresett primer, valamint szekunder források alapján megalkottam a saját fogalom meghatározásomat is. Kutatásom során egyik hipotézisemet, amelyben azt támasztom alá, hogy a kriptovalutával elkövetett bűncselekmények száma növekvő tendenciát mutat, statisztikák, jelentések alapján vizsgáltam. A statisztikákat ábrákban jelenítettem meg, különösen amerikai viszonylatban. Ehhez az IOCTA, valamint az IC3 jelentéseket használtam fel, hogy még specifikusabban tudjam felmérni a jelenlegi állapotot. Álláspontom szerint azért volt fontos ismertetni, hogy ezen deliktumok száma növekvő tendenciát mutat, mert megítélésem szerint ez is azt mutatja, hogy az elkövetők szívesebben valósítanak meg ilyen módon bűncselekményeket, hiszen tisztában vannak vele, hogy ezeknek bebizonyítása nehézséget okoz az eljárásban részt vevőknek.

Dolgozatomban kiemelt jelentőséggel bír, hogy a bizonyítást olyan szemszögből vizsgálom, amely kifejezetten a kriptovalutával elkövetett bűncselekmények speciális blokklánc vizsgálatát mutatja be, összhangban a hatályos magyar büntetőeljárásjogi törvénnyel.

Szemléltetni kívántam továbbá azt, hogy milyen fontossággal bír a felügyeleti lánc ismerete, valamint annak elemzése az igazságszolgáltatás sikerességének fényében. A sikeres ismertetéshez tovább vizsgáltam a lefoglalás kereteit és elveit is, hiszen a lefoglalás a bizonyítékok biztosításának elsődleges módja. A blokklánc vizsgálat, valamint a felügyeleti lánc ismeretéhez, s annak bizonyítási eszközként való funkcionálásának bemutatásához dolgozatomban az interdiszciplinális kitekintés a jellemző. Ahhoz, hogy ezeket a jelenségeket jobban szemléltetni tudjam, számos informatikai elemzést, véleményt ismertem meg, s hoztam összhangba a büntetőeljárásjoggal.

Dolgozatom utolsó szegmenségben összehasonlító elemzést folytattam a magyar, valamint az amerikai szabályozások terén, kutatásom ezen részét a floridai *University of Miami*-n végeztem.

III. Alapfogalmak és elméleti háttér

1. A kiberbűncselekmény (cybercrime) fogalmi értelmezése

A digitális technológia elterjedése, valamint a számítógépes világ gyors fejlődése cáfolhatatlanul megváltoztatta a mindennapi életünket. Megkérdőjelezhetetlen az a tény, hogy ezen jelenségnek vannak jelentős előnyei és hátrányai is. Hátrányok közé sorolandó a kibertérben folyó bűnözés, amelyhez több bűnüldözési szerv együttes, kitartó kooperatív munkájára van szükség, hogy sikeres legyen a bűncselekmények szankcionálása. A kiberbűncselekményre mai napig nem tudunk egy egységes fogalmat kialakítani, hiszen a jogszabályok sajnos sokkal lassabban születnek meg, mint ahogy a technológia fejlődik. Hazai tekintetben sem a 2012. évi C. Törvény (továbbiakban: Btk.), sem a 2017. évi XC. törvény (a továbbiakban: Be.) nem tartalmazza a „cybercrime”¹ fogalmát. A 1139/2013. (III.21.)² Korm. Határozat sem nevezi meg, hogy pontosan mit is értünk a „cybercrime” kifejezés alatt.

Európai és amerikai kitekintésem során is arra jutottam, hogy nincs egységes terminológia kialakítva. Az Európai Bizottság úgy határoz róla, hogy a kiberbűncselekmény olyan határokon átvéelő tág fogalom, ami magában foglalja az internetes bűncselekményeket, az internetes csalást és hamisítást, valamint a jogellenes online tartalmakat is.³ További nézőpontok szerint ide tartoznak a technológia-alapú, a „high-tech”, valamint az e-bűncselekmények is.⁴

Ugyan a kérdéssel az Európai Tanács 2001. évi Budapesti Számítástechnikai Bűnözésről szóló Egyezménye már foglalkozott, de ebben sem jelent meg konkrét fogalomként.⁵

Az Europol, valamint az EC3⁶ értelmezésében a kiberbűncselekmények nem ismernek nemzetközi határokat. A bűnözők kihasználják a számukra rendelkezésre álló technikai eszközöket, valamint több joghatóságot ölel fel ez a bűncselekményfajta. Amerikában a

¹ CYBERCRIME: Az angol kifejezés jelentése: kiberbűncselekmény

² 1139/2013. (III.2.) Korm. Határozat, Magyarország Nemzeti Kiberstratégiájáról. Nemzeti Jogszabálytár. (<https://njt.hu/jogszabaly/2013-1139-30-22> utolsó megnyitás: 2024.09.02.)

³ EURÓPAI BIZOTTSÁG. (2024) Cybercrime. (https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en?prefLang=hu&ettrans=hu utolsó megnyitás: 2024.11.12.)

⁴ BARTKÓ Róbert – SÁNTHA Ferenc: A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre. In: *Military and Intelligence Cybersecurity research Paper*, 2023/2. 4. o. (<https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC%20RP%202023-2%20-%20Bartko%20Rober-Santha%20Ferenc%20-%20A%20kibert%20muveletek%20buntetojogi%20ertelmezese%20lehetosegei.pdf> utolsó megnyitás: 2024.12.03.)

⁵ 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről (<https://net.jogtar.hu/jogszabaly?docid=a0400079.tv> utolsó megnyitás: 2024.10.25.)

⁶ EUROPOL. About Europol. EC3 (2024) (<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> utolsó megnyitás: 2024.09.09.)

„Homeland Security Investigations” úgy rendelkezett róla, hogy a kiberbűnözés minden olyan illegális tevékenységet foglal magába, amelyet Internet vagy számítógép segítségével hajtanak végre.⁷

A legtöbb meghatározásról az mondható el, hogy közös elemeket használnak, de úgy értelmezik a fogalmat, hogy egy olyan törvénysértő cselekmény, amelyet információs és kommunikációs technológia segítségével és felhasználásával követnek el. A bűnelkövetők célja a hálózatok, rendszerek, adatok, webhelyek és technológia felhasználása bűncselekmény elkövetéséhez.

Mindezekből látszik, hogy fontos meghatározni a kiberbűnözés fogalmát, így az alábbi a javaslatom az általam vizsgált szervezetek alapján:

Olyan, illegális cselekményeket magában foglaló, legtöbbször névtelen elkövetők által végrehajtott, az elektronikus hálózatot igénybevevő, ezzel más személyeknek kárt okozó cselekmények sorozata, amelynek elkövetésére gyakran országhatárokon átívelően kerül sor.

Tekintettel arra, hogy jelentős mennyiségű kiberbűncselekmény valósul meg mindennapjainkban, dolgozatom a kriptovalutával elkövetett bűncselekményekre összpontosít. Ezen deliktumok elterjedésére, fajtáira, bizonyítására, valamint ennek nehézségeit szeretném bemutatni. Annak érdekében, hogy jobban megérthessük, hogy mi a kriptovaluta, egy rövid történeti és fogalmi kitekintést kívánok tenni.

2. A kriptovaluták kialakulásának rövid története, működése

A kriptovaluta tipikusan egy olyan rövid történeti múlttal rendelkező jelenség, amelyet klasszikus enciklopédiai környezetben nem találhatunk meg. Ha tágabb kontextusba helyezzük, akkor egy pénzügyi újításról van szó, amelyet a digitalizáció keltett életre.

Forradalmian új ötletnek számított 2008 novemberében Satoshi Nakamoto nyolcoldalas javaslata, amely a Bitcoin nevet kapta a Cryptography levelezőlistán, amely egy potenciális megoldást próbált bemutatni a központi elszámoló felek által működtetett fizetési rendszerhez képest. Ezelőtt a digitális tranzakció csak úgy volt kivitelezhető, hogyha arról másolat keletkezett, s ezt a felek egy harmadik félre (leginkább pénzintézetekre) bízták. A *Bitcoin* nem csak magát a kriptovalutát foglalja magában, hanem egy digitális fizetési rendszert is. Érdemes említést tenni arról, hogy ez egy nyílt forráskóddal rendelkező rendszer, ebből fakadóan a hálózaton végbemenő *Bitcoin* tranzakciókat nyilvános nyomon lehet követni. Ez alatt azt értem,

⁷ U.S. DEPARTMENT OF HOMELAND SECURITY. *Homeland Security Investigations*. (<https://www.dhs.gov/hsi/investigate/cybercrime> utolsó megnyitás: 2024.09.02.)

hogy nem kifejezetten a személyt lehet beazonosítani, hanem a feladó és címzett felekhez kapcsolódó *Bitcoin-címeket*, valamint a tranzakciók összegét a blokkcsatornán. Ebből adódóan, pontos személyt nem minden esetben lehet beazonosítani, hiszen *pseudoanonim* tranzakciókról beszélünk.⁸

Azonban a 2008-ban bekövetkezett válság miatt az emberek bankokba vetett bizalma megingott, s ez odáig fajult, hogy felmerült az igény arra, hogy közvetítő nélküli tranzakciókat alkalmazzanak.⁹ Satoshi célja az volt, hogy létrehozzon egy elektronikus kriptó (kódoláson alapuló) fiskális rendszert. A kihívás abban rejlett, hogy egy olyan módszert kellett találnia, amelyben biztosított volt az, hogy az adott pénzegység csak egyszer legyen felhasználható, így akarta a hamisítás lehetőségét kizárni. Így született meg a *peer-to-peer* megoldás, amely úgy valósul meg, hogy mindenki számára nyitott és elérhető hálózatokon zajlanak a tranzakciók, azok hitelesítése.

A menete az alábbi folyamat:

1. A tranzakciót elindító bejelenti a tranzakciós szándékát, s ezt a teljes közösség előtt teszi, lényeges információkat oszt meg, s egyedi azonosítóval látja el, ezt követően a hálózat tagjai hitelesítik a tranzakciót.

2. A forradalmi része azonban a következő lépésben lelehető meg: a tranzakció hitelesítését a szabadpiaci alapokra helyezve érdekeltté teszi benne a hálózaton lévőket és versenyezteti őket.

3. Ez hogyan valósul meg? A hitelesítéshez használt véletlenszerűen generált „hashkódok” nagy erőforrásigényes visszafejtésének elvégzése után az abban részt vett tagok jutalomban részesülnek. Ez kriptovaluta-bányászatként lehet ismerős.¹⁰

Ahhoz, hogy az utalás megtörténjen, kétféle kulcsra van szüksége a felhasználónak, egy nyilvános, valamint egy privát kulcsra. A privát kulcs egy jelszóként funkcionál, s ennek ismerete azért szükséges, mert ez biztosítja azt, hogy az adott egységeink felett rendelkezessünk, valamint, hogy utalást végezhessünk. Ezen kulcspár közreműködésével utalhatunk az ún. virtuális tárcákba, amelyek digitális adatok, s ezek blokkláncba fűzve

⁸ MEZEI Kitti: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban, In: *Pro Futuro*, 2019./1., 80. o. (<https://ojs.lib.unideb.hu/profuturo/article/view/3906/5176> utolsó megnyitás: 2024.09.15.)

⁹ JÁMBOR Gellért: A kriptovaluták megjelenése, elterjedése és a jelenséggel szemben lehetséges jogi lépések, In: *Magyar Rendészet*, 2023./4., 116. o.

¹⁰ NAKAMOTO Satoshi (2008) Bitcoin: A peer-to-peer electronic cash system. (<https://assets.pubpub.org/d8wct41f/31611263538139.pdf> utolsó megnyitás: 2024.09.15.)

helyezkednek el.¹¹ Funkciója abban nyilvánul meg, hogy a privát kulcsot létrehozza, illetve tárolja.¹²

Összegezve, Satoshi Nakamoto által megálmodott hitelesítési rendszer lett az összes kriptovaluta alapja, amely nem más, mint a blokklánc.¹³ A blokklánc lényegében egy decentralizált vagy megosztott főkönyv, amely a kriptográfiai eljárásoknak köszönhetően alkalmas a tranzakciók hitelesítésére, de ezt olyan módon teszi, hogy nem kell hozzá hitelesítő szerv vagy személy.¹⁴ Az adatok a blokkláncban blokkokra vannak osztva, amelyeket egyedi azonosítókkal látnak el, ide sorolandó az időbélyeg és a digitális aláírás.¹⁵

Jelen téma szempontjából azért volt fontos kitérnem arra, hogy a blokklánc megosztott főkönyvként funkcionál – amely azt jelenti az Európai Parlament és a Tanács (EU) 2022/858. rendelete alapján, hogy az ügyletek nyilvántartását foglalja magába, a DLT-hálózati csomópontként adott körében egy konszenzusos mechanizmus alkalmazásával szinkronizált, valamint egy megosztott adattár¹⁶, s a számítógépek megosztott hálózatán keresztül, az összes tranzakciót rögzíti¹⁷ – mert a bizonyítás szempontjából fontos lesz a dolgozat későbbi részében.

¹¹ SIMON Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások, In: MEZEI Kitti (szerk.:) *A bűnügyi tudományok és az informatika*, Pécs, Magyarország, Budapest, Magyarország: PTE ÁJK, MTA Társadalomtudományi Kutatóközpont, 2019, 173. o. (https://jog.tk.hun-ren.hu/uploads/files/09_buntetojog_informatika_SIMONB.pdf) utolsó megnyitás: 2024.09.16.)

¹² MEZEI Kitti: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban, In: *Pro Futuro*, 2019./1., 81. o. (<https://ojs.lib.unideb.hu/profuturo/article/view/3906/5176>) utolsó megnyitás: 2024.09.15.)

¹³ NAKAMOTO Satoshi (2008) Bitcoin: A peer-to-peer electronic cash system. (<https://assets.pubpub.org/d8wct41f/31611263538139.pdf>) utolsó megnyitás: 2024.09.15.)

¹⁴ KIRÁLY Péter Bálint: A blokklánc-technológia nemzetközi kereskedelmi jogi összefüggései. In: *Külgazdaság*, 2019./3-4., 19. o.

¹⁵ GÁBOR Tamás – KISS Gábor Dávid: Bevezetés a kriptovaluták világába, In: *Gazdaság és Pénzügy*, 2018./1., 38. o.

¹⁶ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022/858 Rendelete, 2022. május, 2.cikk, Fogalommeghatározások, 2. (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32022R0858>) utolsó megnyitás: 2024.09.13.)

¹⁷ VARGA Norbert – BIRHER Nándor – KNOLL-CSETE Edit: A kriptovaluták szabályozása-Jogi kihívások és kockázatok. In: *Humán Innovációs Szemle* 2024./1., 5. o. (<https://ojs.ppke.hu/hisz/article/view/1161/1217>) utolsó megnyitás: 2024.09.14.)

3. A kriptovaluták fogalmi köre

A következő fogalmak tisztázása azért fontos, mert az EU 2023/1114. Európai Parlament és Tanácsi rendelet¹⁸, azaz a MiCA (*Markets in Crypto-Assets Regulation*) pontosítja a kriptovalutákra vonatkozó meghatározásokat, amely lehetővé teszi a kriptoeszközökkel kapcsolatos szabályozás egységesítését az EU-ban. Kiemelendő, hogy a Magyar Nemzeti Bank becslései szerint már mintegy 200.000 személy rendelkezik virtuális kriptoeszközzel, amely jól mutatja azt, hogy a befektetők köre folyamatosan nő. A növekedésnek köszönhetően a kriptoeszközök kockázatosnak számítanak, hiszen rengeteg esetben valósulnak meg bűncselekmények, mint például csalás, lopás, pénzmosás.¹⁹

E rendeletnek, valamint az uniós jogharmonizációnak köszönhetően Magyarországon a 2024. évi VII.²⁰ törvény foglalja magában a kriptoeszközökkel kapcsolatos felügyeleti szabályokat. Az általam ismertetni kívánt fogalmakat alkalmazzák az előbb említett törvényben is.

1. Kriptoeszköz a rendelet értelmében egy olyan érték vagy jog digitális megtestesítője, amely megosztott főkönyvi technológia vagy hasonló technológia alkalmazásával elektronikusan egyaránt átruházható és tárolható.

2. Eszközalapú token alatt a kriptoeszközök egy olyan típusát értjük, amely nem elektronikuspénz-token, és amely stabil érték fenntartására törekszik, hogy másik értékhez vagy joghoz, vagy ezek kombinációjához van kötve, beleértve egy vagy több hivatalos pénznemet is.²¹

A kriptovaluták nem tekinthetők pénzeszköznek, de törvényesen át-, továbbá visszaválthatóak, valamint más kriptoeszközre is át lehet váltani – mondta ki a MiCA rendelet.²²

Kiemelendő, hogy egy decentralizált rendszerről van szó. Ez azt jelenti, hogy közvetítő beiktatása nélkül is működik, így a felhasználók egymás között tudják lebonyolítani a tranzakciókat. A decentralizáció éppen ezért jelent hatalmas veszélyforrást, mert nem minden kriptoeszköz tekintetében küszöbölhető ki az anonimitás, mint probléma. A Bitcoin esetében a

¹⁸ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2023/1114. Rendelete, 2023. május (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32023R1114> utolsó megnyitás: 2024.09.14.)

¹⁹ MAGYAR NEMZETI BANK: Sajtóközlemény, 2024.04.11. (<https://www.mnb.hu/sajtoszoba/sajtokozlomenyek/2024-evi-sajtokozlomenyek/fokozott-befektetoi-kockazattal-jarhatnak-a-kriptoeszkozok-kriptotozsdek> utolsó megnyitás: 2024.09.20.)

²⁰ A kriptoeszközök piacáról szóló 2024. évi VII. Törvény. (<https://njt.hu/jogszabaly/2024-7-00-00> utolsó megnyitás: 2024.09.30.)

²¹ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2023/1114. Rendelete. 2023. május, 3. cikk, Fogalommeghatározás: 5., 6., 7. (<https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32023R1114&qid=1693071757416> utolsó megnyitás: 2024.09.14.)

²² Uo. 3. cikk, Fogalommeghatározás: 19. és 20. pontja.

tranzakciók alapvetően nyomon követhetőek, mivel a blokklánc ezt az esetek nagyrésztében biztosítja, de például vannak olyan érmék, amelyeket nagyobb kihívás lenyomozni, hiszen egy olyan céllal hozták létre, hogy egy teljesen privát hálózatot teremtsen a használók számára.²³

Továbbá egy független rendszerről van szó, hiszen egyetlen ország jegybankja sem áll a rendszerek mögött, sokkal inkább beszélhetünk egy felhasználók közötti „bizalmi” megegyezésről.²⁴

Valamint az anonimitás is az egyik legfontosabb jellemzője. Részben ezért is okoz kihívást a bizonyítás kérdése egy felmerülő büntetőeljárásban, hiszen ezek az érmék nem névre szólóak, egy személy sem kapcsolható közvetlenül valamely tárcához, illetve tranzakcióhoz. Egyetlen tulajdonság dönt a kriptovaluta használhatóságában, mégpedig az, hogy ki fér hozzá a titkosítási kulcshoz, miközben az utolsó azzal végzett tranzakció címzettjeként jegyezték be az adott érmehez tartozó blokkláncban. Jelentős különbség az, hogy minden kriptovaluta esetében eltér az anonimitás foka.²⁵

Összességében levonható az a következtetés, hogy az uniós elvárásoknak megfelel a magyar jogi szabályozások. Ugyanakkor ezen szabályozásnak mind hazai, mind nemzetközi szinten fejlődnie kell még, hogy a jövő kihívásával sikeresen szembe tudjunk nézni.²⁶

²³ BÁCSKAI Máté: A kriptovaluták büntetőjogi értelmezése a pénzmosás és a lopás tükrében. In: *Ügyészek Lapja*, 2024./1., 103-110. o.

²⁴ MEZEI Kitti: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban, In: *Pro Futuro*, 2019./1., 80. o. (<https://ojs.lib.unideb.hu/profuturo/article/view/3906/5176> utolsó megnyitás: 2024.09.15.)

²⁵ DORNFELD László: A kriptovaluták és az e-bizalom kapcsolata, In: *Magyar Rendészet*, 2021./4., 219. o.

²⁶ POLT Péter: Digitális fejlődés és büntetőjog – akkor és most. In: *Belügyi Szemle*, 2022./11., 2392. (<https://belugyiszemlejournal.org/index.php/belugyiszemle/article/view/1140/1141> utolsó megnyitás: 2024.12.01.)

IV. Kriptovalutákkal leggyakrabban elkövetett bűncselekmények az Európai Unióban

Az Europol az általa 2024-ben kiadott IOCTA²⁷ jelentésében mutatta be az internetes, szervezett bűnözés veszélyeit, valamint értékelte is azokat. A IOCTA dokumentum alátámasztja azon tézisémet, hogy a kriptovalutákkal elkövetett bűncselekmények száma nő, és azt is, hogy felhasználási körük is egyre szélesebb. Ezen felül az Europolhoz érkező kriptovalutával összefüggő nyomozási cselekményeinek támogatására is nőtt az igény.²⁸

A kriptovaluták esetében a befektetési csalások jelentik a legnagyobb veszélyt továbbra is, valamint egyre többször alakítják át a Bitcoint más, stabil érmékre – számoltak be erről a nyomozók. A stabilérmék bizonyos része feketelistát tartalmaz a „smart contract”-ban, ami lehetővé teszi azt, hogy a jogalkalmazó szervek felszólítsák a cégeket arra, hogy fagyasszák be a stabilérméiket, amelyek a gyanúsított pénztárcájának részét képezik. Kiemelendő újtásnak gondolom azt, hogy a kriptoeszköz-szolgáltatók esetében is a pénzeszközök átutalását kísérő információkra jelentési kötelezettséget terjesztettek az Európai Unióban, s 2024. januárjában elfogadták.

A pénzmosás és a terrorizmus-finanszírozás is elterjedt bűncselekmények közé tartozik. A különböző bűncselekményekből befolyt összegeket – az anonimitásnak köszönhetően – itt tudják a legkönnyebben „tisztára mosni”, vagy éppen a terrorista cselekményeket finanszírozni, majd különböző címekre vagy személyekhez eljuttatni.²⁹

További problémákat vet fel a zsarolás, amely alapvetően egy klasszikus bűncselekménynek minősül, ez esetben annyi különbséggel, hogy zsarolóprogramokról van szó, amelyek Bitcoint kérnek többnyire váltságdíjként, de vannak esetek, amikor más altcoinokat (kevésbé ismert, alternatív) követelnek.³⁰

Végül a piramisjáték szervezése említendő, ahol a befektetők virtuális fizetőeszközökbe invesztálnak, amelyek gyorsan ígérnek nagy hozamot. A hagyományos piramisjátékra alapozva csálnak ki óriási összegeket a befektetőktől többnyire offshore cégek. Itt példaként említem a *Onecoin*, amely Ruja Ignatova nagyszabású csalási programja volt. Dollármilliókat csalt ki

²⁷ IOCTA: Internet Organised Crime Threat Assessment,

²⁸ IOCTA: Europol (2024), Internet Organised Crime Threat Assessment (IOCTA), Publications Office of the European Union, 6. o. (<https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> utolsó megnyitás: 2024.10.09.)

²⁹ MEZEI Kitti: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban, In: *Pro Futuro*, 2019./1., 87. o. (<https://ojs.lib.unideb.hu/profuturo/article/view/3906/5176> utolsó megnyitás: 2024.09.15.)

³⁰ IOCTA: Europol (2024), Internet Organised Crime Threat Assessment (IOCTA), Publications Office of the European Union, 13. o. (<https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> utolsó megnyitás: 2024.10.09.)

emberekből a bolgár székhellyel rendelkező vállalat. Ruja Ignatova az „áldozatait” arra kérte, hogy utaljanak befektetési alapokat *Onecoin* számlákra azért, hogy majd onnan *Onecoin* csomagokat vásárolhassanak.³¹

³¹ FEDERAL BUREAU OF INVESTIGATION (2024) FBI Ten Most Wanted Fugitive. Ruja Ignatova. (<https://www.fbi.gov/wanted/topten/ruja-ignatova/@@download.pdf> utolsó megnyitás: 2024.10.09.)

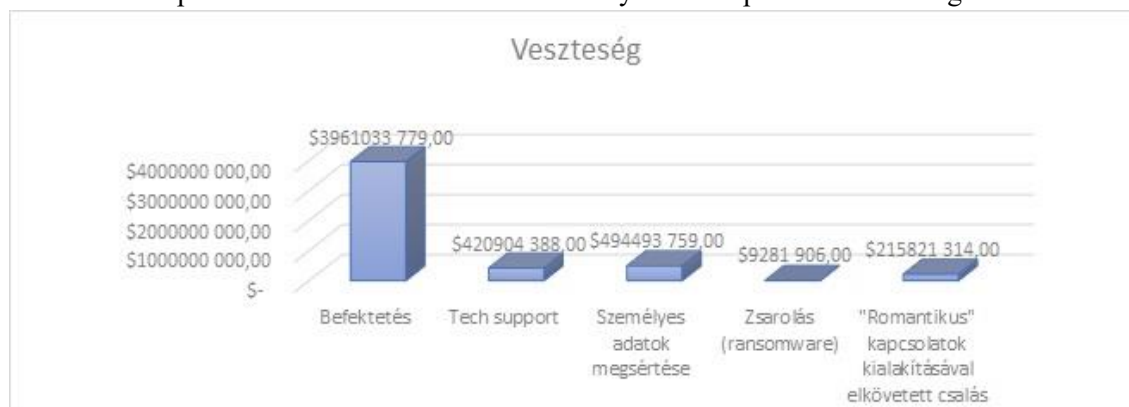
V. Kriptovalutákkal leggyakrabban elkövetett bűncselekmények az USA-ban

Az Egyesült Államokban az FBI³² egyik divíziója, az IC3³³ (*Internet Crime Complaint Center*) foglalkozik részletesebben a kriptobűncselekményekkel. Éves jelentésben, statisztikákkal, valamint különböző elemzési szempontok (*kor, bűncselekmények, elkövetők*) alapján hívják fel a figyelmet a potenciális veszélyforrásokra. A 2023-as évben összesen 69,468 panasz érkezett, ami 5,6 milliárd USD veszteséget összesített.³⁴A veszteségek száma közel 45%-kal nőtt 2022-es évhez képest.

1. táblázat: Kriptovalutával elkövetett bűncselekmények bejelentéseinek megoszlása az USA-ban

Kriptovalutával elkövetett bűncselekmények	Bejelentések száma
Befektetés	32094
Tech support	8719
Személyes adatok megsértése	8716
Zsarolás (ransomware)	8630
Romantikus kapcsolatok kialakításával elkövetett csalás	3749

1. ábra: Kriptovalutával elkövetett bűncselekmények miatti pénzübeli veszteségek az USA-ban³⁵



Dolgozatom e szakaszában tételesen csak a kriptovalutákkal elkövetett befektetési csalással foglalkozom, hiszen az általam elkészített ábrából is jól látszik, hogy a legtöbb veszteséget ezen bűncselekmény megvalósulása okozta, amely közel 4,000,000,000 USD volt.

³² FBI: *Federal Bureau of Investigation*

³³ IC3: *Internet Crime Complaint Center*, melynek célja, hogy a nyilvánosság számára megbízható bejelentési mechanizmust biztosítson az FBI számára, az interneten elkövetett bűncselekményekkel kapcsolatos információk benyújtásához.

³⁴ FEDERAL BUREAU OF INVESTIGATION, Internet Crime Complaint Center (2024) 2023. IC3 Cryptocurrency Report. 4. o. (https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf utolsó megnyitás: 2024.10.18.)

³⁵ Uo. 7. o.

2023-ban a befektetési csalásoknak az egyik legkedveltebb taktikája volt az, hogy az áldozatokkal „romantikus” kapcsolatot próbálnak meg kialakítani (pl.: ismerkedéssel kapcsolatos applikációkban), bizalmukba próbálnak férközni. Miután ezt elérték, bemutatnak egy kripto befektetési lehetőséget. Miután már kialakult az áldozat részéről a kötődés, illetve a bizalom, az esetek nagyrésztében befektetést kezdenek csaló, hamis weboldalakon, ahol az elkövető hamis profitokat mutat az áldozatoknak. Eleinte tényleg kisebb profitot észlelnek az áldozatok, és ez tovább bátorítja őket arra, hogy még több pénzt fektessenek be.³⁶

Népszerű befektetésnek tűnhetett a likvidbányászás is. Ez egy olyan stratégia, ami passzív jövedelmet ígér a kripto által. Alapesetben a befektetők kriptovalutáikat egy likviditási medencébe kötik, és a kereskedők számára a tranzakciók lebonyolításához szükséges valutákat biztosítják. A csalást elkövetők köre ezen változatban kihasználja a kriptovaluta tulajdonosát/tulajdonosait, ráveszik arra, hogy vágjon bele befektetési lehetőségbe, de úgy, hogy kapcsolják össze a profiljukat egy kriptotárcával. A csalók ezután a befektetni kívánt összeget bármiféle értesítés nélkül törlik.³⁷

Az utolsó bűncselekmény, amelyet bemutatok ebben a szakaszban, az nem más, mint a *play-to-earn game*. Az FBI külön felhívást adott ki 2023.03.09-én (I-030923-PSA), hogy csalók millió dollárokat lopnak el kriptovalutában különböző játékokból. Itt is hasonló séma merül fel, mint az előző esetekben. Az áldozatokkal kapcsolatot építenek ki, majd ráveszik, hogy töltsse le az alkalmazást, amely által pénz nyerhetnek. Hasonlóan kriptopénztárcát kell létrehozniuk, ahová a játékhoz szükséges pénzt be tudják fizetni. A csalók egy rosszindulatú program által ellopják az áldozatok pénzét, s azzal magyarázzák, hogy majd visszaigényelhetik pénzüket további adók megfizetésével.³⁸

Összegezve elmondható, hogy a kriptovalutával elkövetett bűncselekmények száma növekvő tendenciát mutat, az általam vizsgált jelentések alapján ez jól látszik. Mivel ezen bűncselekmények száma nő, így köthető első hipotézisem össze a másodikkal, amelyben feltételezem, hogy ezen bűncselekmények bizonyítása nagyobb kihívás elé állítja az eljáró hatóságokat, így a következő fejezetekben a hagyományos bizonyításelmélet mellett kívánom bemutatni a bizonyítás új dimenzióját a kriptovaluták fényében.

³⁶ Uo. 13. o.

³⁷ Uo. 7., 14. o.

³⁸ FEDERAL BUREAU OF INVESTIGATION, (2024) *Public Service Announcement: Emerging threat to personal safety*. Internet Crime Complaint Center. I-030923-PSA. (<https://www.ic3.gov/PSA/2023/PSA230309> utolsó megnyitás: 2024.10.18.)

VI. A hagyományos bizonyításelmélet

Tekintettel arra, hogy ezen dolgozat az elektronikus adat bizonyítási eszközként való felhasználásával foglalkozik, különös tekintettel a kriptovaluták körében, így nem mehetünk el amellett, hogy a hagyományos bizonyításelméletet is bemutassam röviden. Ennek tükrében kaphatunk egy átfogó képet arról, hogy honnan hová jutottunk el a digitalizáció adta újabb kihívások mentén.

Király Tibor szavaival élve „*a bizonyítás komplex jelenség, amely magában hordozza a bíróság, az ügyész és a nyomozó hatóság, valamint az eljárás többi résztvevőjének megismerő tevékenységét, a logikai bizonyítást, és ezeknek a logikailag szabályozott rendjét.*”³⁹

Ezen megfogalmazás, csak egy a sok fogalmi meghatározás közül. Egységes terminológia aligha született, de egy visszatérő elem mindig jelen volt, amely nem más, mint a logika fontossága.⁴⁰

A bizonyítás egy sajátos megismerési folyamat, amelynek célja a múltban történő események lehető legpontosabb feltárása mellett, a bizonyítási eszközök felderítése, összegyűjtése, továbbá biztosítása és felhasználása, valamint a bizonyítási eszközök alapján elérhetővé vált bizonyítékok összehasonlítása.⁴¹ A bizonyítási eszköz tehát, a bizonyítékok hordozója, a bizonyíték pedig az az információ, amelyhez a bizonyítási eszköz révén jutunk.⁴²

A bizonyítási eljárás pedig az a speciális folyamat, amelyben a jogalkalmazó szerveknek célja, hogy az adott szerv hatáskörébe tartozó ügy eldöntéséhez nélkülözhetetlenül releváns tényeknek, valamint adatoknak a birtokába kerüljön. A bizonyítási eljárás három alrendszerben határozható meg: információs, ténybeli, valamint a hipotetikus alrendszer. A prekonceptió, azaz a hipotézis immanens része a bizonyítási eljárásnak, hiszen az eljárás előre mozdításának szükséges eleme. Ha az eljáró hatóság vagy a bíró nem rendelkezne előzetes feltevésekkel az ügygel kapcsolatban, nem tudná ellátni a jogalkalmazói feladatát.⁴³ Alapvető vonatkozásban azonban fontos kiemelni, hogy a prekonceptió nem mutatkozhat meg nyíltan, hiszen abban az esetben a tisztességes eljárás elvét elfogultság miatt sértené.⁴⁴

³⁹ KIRÁLY Tibor: *Büntetőeljárás jog*. Budapest, Osiris Kiadó, 2003, 222. o.

⁴⁰ BÉRCES Viktor: *A büntetőeljárás reformja és a bizonyítás alapkérdései*, Budapest, ELTE Eötvös Kiadó, 2021, 49. o.

⁴¹ BELOVICS Ervin - BÉRCES Viktor: *Büntető eljárásjog*, Budapest, Orac Kiadó, 2023, 224. o.

⁴² SORBÁN Kinga: A digitális bizonyíték a büntetőeljárásban, In: *Belügyi Szemle*, 2016./11., 82. o.

⁴³ BELOVICS - BÉRCES i. m. 226. o.

⁴⁴ BELOVICS - BÉRCES i. m. 227. o.

A bizonyítás rendeltetése tehát nem más, mint a büntetőjogi felelősség eldöntéséhez szükséges relevanciával bíró tények, valamint tudás megszerzése, feladata pedig az elkövetett deliktum vonatkozásában a tényállás tisztázása.⁴⁵

A digitális bizonyíték felhasználása a bizonyítás egy teljesen új aspektusát mutatták be az utóbbi évtizedben. Annak érdekében, hogy a bizonyítás sikeres legyen, a bizonyítékok összegyűjtésére az ENISA (Európai Unió Kiberbiztonsági Ügynökség) öt nélkülözhetetlen alapelvet fogalmaz meg, amelyek az adatok integritása, a visszakövethetőség, a szakemberek támogatása, a megfelelő képzés, valamint a legalitás.⁴⁶ Hiszen ezek az adatok bizonyító erejüket csak úgy képesek megőrizni, hogyha megtartják azon állapotukat, amely a beszerzésük előtt fennállt.

VII. Az elektronikus bizonyíték fogalmi meghatározásának fejlődése

Az elektronikus bizonyíték fogalmát az Európa Tanács már a 2001-es számítástechnikai bűnözésről szóló Budapesti Egyezményben is említi, de mint fogalom nem fejtette ki.⁴⁷

2016-ban az Európai Tanács következtetéseket fogadott el a kibertérben gyakorolt büntető igazságszolgáltatás javításáról. Ennek keretében hangsúlyozta, hogy az elektronikus bizonyítékok egyre fontosabb szerepet játszanak a büntetőeljárásokban minden típusú bűncselekmény, különösen a terrorizmus esetében.⁴⁸

2017 júniusában az Európai Tanács úgy vélekedett, hogy az elektronikus bizonyítékokhoz való tényleges hozzáférés kiemelkedően jelentős a súlyos bűncselekmények elleni küzdelemben.⁴⁹ Ugyanebben az évben a Tanács következtetéseket fogadott el azügyben, hogy az Európai Unióban egy erőteljes, kimagasló kiberbiztonsági rendszert tudjon kiépíteni. A Tanácsi következtetésben már a bevezetésben kiemeli, hogy exponenciálisan nő a kockázat, valamint, hogy nagy hangsúlyt kell fektetni a kiberbiztonságra.⁵⁰ A II. fejezet 46-47. részében

⁴⁵ BODNÁR Péter András: A digitális bizonyítékok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. In: *Büntetőjogi Szemle*. 2021./1. 23. o.

⁴⁶ EUROPEAN UNION AGENCY FOR CYBERSECURITY (2014) *Electronic Evidence: A basic guide for first responders*. 5. o. (https://www.era-comm.eu/EPPO/kiosk/pdf/ENISA_2014.pdf utolsó megnyitás: 2024. 10. 03.)

⁴⁷ 2004. évi LXXIX. Törvény az Európa Tanács Budapest, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről (<https://net.jogtar.hu/jogszabaly?docid=a0400079.tv> utolsó megnyitás: 2024.10.25.)

⁴⁸ AZ EURÓPAI UNIÓ TANÁCSA. *Az Európai Unió kiberbiztonsági stratégiája: A kiberbiztonság, mint a nemzetközi biztonság alapvető eleme.*, 2016. 3. o. (<https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf> utolsó megnyitás: 2024.10.25.)

⁴⁹ AZ EURÓPAI TANÁCS. *Az Európai Tanács következtetései*, 2017, 2. o. (<https://www.consilium.europa.eu/media/23972/22-23-euco-final-conclusions-hu.pdf> utolsó megnyitás: 2024.10.25.)

⁵⁰ AZ EURÓPAI UNIÓ TANÁCSA. *A kiberbiztonságról szóló következtetések*, 2017, 2. o. (<https://www.consilium.europa.eu/media/31666/st14435en17.pdf> utolsó megnyitás: 2024.10.15.)

kifejezetten támogatja azokat a munkafolyamatokat, amelyek az elektronikus bizonyítékok határon átnyúló hozzáféréseivel kapcsolatosak, valamint kihangsúlyozza, hogy ezeknek megszerzése a hatóságok részéről semmilyen szinten sem lehet jogsértő, valamint tiszteletben kell tartaniuk az alapvető emberi jogokat. Továbbá a Bizottságtól egy előrehaladási tervet is kértek, amely tartalmazta azokat a végrehajtási gyakorlati intézkedéseket, amelyek szükségesek voltak ahhoz, hogy az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférést javítsák, illetve ehhez egy jogalkotási javaslatot is kérvényeztek.⁵¹

A fogalmi hiányosság felismerésére először a 2018-as e-bizonyíték javaslatban került sor, amely a Bizottság azon közzétett javaslatcsomagja, amely egy rendeletjavaslatot, valamint egy irányelvet tartalmazott. Tulajdonképpen egyetlen területre fektet hangsúlyt, amely az elektronikus bizonyítékok határon átnyúló beszerzése. A javaslat kifejezetten épít az európai nyomozási határozatra. Említésre méltó, hogy a javaslat megkönnyíti a hatóságok munkáját olyan tekintetben, hiszen közvetlenül kereshetik meg az eljáró hatóságok az EU-ban a szolgáltatást nyújtó adat tulajdonosát.⁵² Az említett javaslatcsomagban a következőképp határoztak:⁵³

Elektronikus bizonyítéknak felel meg minden, ami elektronikus formában tárolt előfizetői, tranzakciós, hozzáférési és tartalmi adatokat foglal magában, állapítottam meg a rendeletjavaslat 2. szakasz (6) bekezdése alapján.

2019-ben a Bizottság tárgyalta az elektronikus bizonyítékokra irányuló nemzetközi megállapodásokról, valamint 2022-ben a tanács felhatalmazta a tagállamokat a nemzetközi megállapodás aláírására.⁵⁴

Az Európai Parlament és a Tanács (EU) 2023/1543. rendelete is kifejti az elektronikus bizonyíték fogalmát, de ezt a dolgot későbbi szakaszában részletesebben is ismertetem.

Annak érdekében, hogy kutatásom szélesebb körben folytathassam, az amerikai gyakorlatot is vizsgáltam. Az angolszász jog régóta elismeri bizonyítási eszközként az elektronikusan tárolt információt, valamint ismerteti a digitális bizonyíték fogalmát is.⁵⁵ Az egyik megközelítés szerint a digitális bizonyíték, olyan információkat tartalmaz vagy továbbít

⁵¹ AZ EURÓPAI TANÁCS. *Az Európai Tanács következtetései*, 2017, 13. o. (<https://www.consilium.europa.eu/media/23972/22-23-euco-final-conclusions-hu.pdf> utolsó megnyitás: 2024.10.15.)

⁵² DORNFIELD László: A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az EU-ban, In: *Infokommunikáció és Jog*. 2017./2., 37-43. o.

⁵³ Uo. 37-43. o.

⁵⁴ AZ EURÓPAI UNIÓ TANÁCSA. *Az e-bizonyíték idővonala*, 2024, (<https://www.consilium.europa.eu/hu/policies/e-evidence/timeline-e-evidence/> utolsó megnyitás: 2024. 10.15.)

⁵⁵ SORBÁN Kinga: A digitális bizonyíték a büntetőeljárársban, In: *Belügyi Szemle*, 2016 /11., 81. o.

bináris formában, amelyre a bíróságon lehet hivatkozni.⁵⁶ Casey úgy értekezett róla, hogy az elektronikus bizonyíték minden olyan bizonyító erővel bíró adat, vagy információ, amelyet a számítógép segítségével továbbítanak vagy tárolnak.⁵⁷

Az FBI egy 2014-ben kiadott értelmezésében azt taglalja, hogy a digitális bizonyíték egy olyan adat, amelyet azzal a szándékkal szereznek be, hogy a nyomozás során vitatott tényt bizonyítani vagy cáfolni tudják, amelyet bináris formában tárolnak vagy továbbítanak. Digitális bizonyítékok közé sorolják pl.: a számítógépeket, a mobiltelefonokat, chipeket, CD-ket, amelyek a digitális adatot tárolják vagy dolgozzák fel. Az OTD (*Operational Technology Division*), valamint a CPO (*Corporate Policy Office*) azok a szervek, amelyek az FBI digitális bizonyíték programért felelős.⁵⁸

Az elektronikus bizonyítékok megőrzése és beszerzése egyre fontosabb szerepet tölt be az egész Európai Unió területén a nyomozási és bizonyítási eljárások szempontjából. Ennek érdekében az Európai Parlament és a Tanács 2023/1543-as rendeletében fogalmazta meg, hogy milyen célérésekkel szeretné javítani a fennálló helyzetet. Kiemeli, hogy a digitális bizonyítékok beszerzésénél kiemelt figyelmet kell fordítani az EUSZ 6. cikkében lefektetett és a Charta (*Az Európai Unió Alapjogi Chartája*) által megfogalmazott alapvető jogokra és elvekre, a jogszerű eljárásnak, valamint a személyes adatok védelme és a közlések bizalmasságának elvére.⁵⁹

Hangsúlyozta azt, hogy a legfőbb cél azon módszer megtalálása, amellyel kivitelezhető az elektronikus bizonyítékok minél gyorsabb beszerzése és biztosítása.⁶⁰

⁵⁶ NOVAK, Martin – GRIER, Jonathan – GONZALES, Daniel: New approaches to digital evidence acquisition and analysis, 2018. In: *NIJ Journal*, 280.sz. 1. o. (<https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis>) utolsó megnyitás: 2024.11.11.)

⁵⁷ CASEY, Eoghan: *Digital evidence and computer crime*, USA, Elsevier, 2011, 7. o.

⁵⁸ FEDERAL BUREAU OF INVESTIGATION. (2014) *Digital Evidence Policy Guide, Part 01*. Federal Bureau of Investigation. 3. o. (<https://vault.fbi.gov/digital-evidence-policy-guide/digital-evidence-policy-guide-part-01-of-01/view>) utolsó megnyitás: 2024.11.04.)

⁵⁹ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2023/1543. Rendelete (2) bekezdés (<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32023R1543>) utolsó megnyitás: 2024.10.31.)

⁶⁰ Uo. (6) bekezdés

VIII. Az elektronikus adat, mint bizonyíték

A kibertér megjelenésével rengeteg új bűncselekmény terjedt el, valamint a korábban megjelent bűncselekmények egyes szegmenseit az elektronikai vívmányok segítségével könnyebben tudják megvalósítani az elkövetők.⁶¹ Ennek jelentőségét az új büntetőeljárásjogi törvény jogalkotói is helyesen felmérték. Ennek köszönhetően a 2017. évi XC. a bizonyítás eszközei közé sorolja (Be. 165.§) a tanúvallomást, a terhelt vallomását, a szakvéleményt, a pártfogó felügyelői véleményét, a tárgyi bizonyítási eszközt, valamint a témám szempontjából releváns elektronikus adatot is.⁶²

A törvény indokolása megemlíti, hogy azért is vezették be, mert a jogalkotó kifejezett céljának minősült egy olyan büntetőeljárás kialakítása, amely a jövő kihívásaira is képes választ adni.⁶³

A kiberbűncselekmények esetében, azon belül is a kriptovalutákkal elkövetett bűncselekményeknél, azok nyomozási folyamata során nagy számú országhatárokon átnyúló kérelmezési igény keletkezik a bizonyíték szolgáltatásával kapcsolatban, és ezek az elektronikus adatok sokszor digitális bizonyítékként is szolgálnak. Véleményem szerint így kifejezetten jó meglátás volt a jogalkotók részéről, hogy az elektronikus adatot is bizonyítási eszköznek tekinti. Ez is azt mutatja, hogy a jogalkotó az angolszász megoldást implementálta, ahol már régóta elfogadott az elektronikus adat, mint bizonyíték.

IX. A blokklánc technológia hogyan használható fel a bizonyításban?

A digitális kriminalisztika egyik legnagyobb kérdéskörét foglalja magában a digitális bizonyítékok kezelése. A digitális bizonyítékok elemzésével és bemutatásával a *Digital Forensics Science* foglalkozik, amely a jogtudomány és az informatika határán foglal helyet. Olyan módszereket tartalmaz, amelyeknek célja az, hogy a jogi eljárásokat hiteles információval lássák el, hogyha az eljárás részét képezi az elektronikus adat is.⁶⁴ Tekintettel arra, hogy a kriptovaluták nyomozása, valamint a bizonyítékként való megőrzése kihívások elé

⁶¹ DORNFELD László: Az elektronikus bizonyítékszerzés aktuális kérdései, In: *Kriminológia Közlemények*. 2017, 242. o. (https://www.kriminologia.hu/files/kiadvany/2019/16_dornfeldl.pdf utolsó megnyitás: 2024.10.04.)

⁶² 2017. évi XC. tv. Be 165.§ a-f)

⁶³ RÓTH Erika: Az elektronikus adat, mint új bizonyítási eszköz megjelenése a büntetőeljárásjogi törvényben, In: *Miskolci Jogi Szemle*, 2020./3., 167. o. (https://www.mjsz.uni-miskolc.hu/files/13834/19_rótherika_tördelt.pdf utolsó megnyitás: 2024.10.04.)

⁶⁴ BODNÁR Péter András: A digitális bizonyítékok megjelenése a büntetőeljárásban – különös tekintettel a szakértői igénybevételére. In: *Büntetőjogi Szemle*. 2021./1., 27. o.

állítják az ebben részt vevő feleket, az eljárást számos kereskedelmi és nem kereskedelmi elemző támogatja, amelyek a blokklánc-átláthatóságát próbálják biztosítani.⁶⁵

Peszleg kiemeli, hogy meghatározó erővel bír a digitális bizonyítékot érintő beszerzési folyamatoknál az, hogy törvényes kereteken belül, szakszerűen történjen meg a beszerzés, valamint az, hogy a zárt bizonyítási lánc érintetlen állapotban legyen.⁶⁶

A 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezmény 1. Cikk b) pontja határozza meg a számítástechnikai adat fogalmát, ez alapján határozza meg a Be. is.

„(1) Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”⁶⁷

A fogalomból a kriptovaluták esetében a program szót érdemes megvizsgálnunk, hiszen a valuták működését különböző szoftverek segítik elő. Ennek fényében a következő megállapításra jutottam. A blokklánc-technológia, mint bizonyíték azért használható fel, mert képes arra, hogy szekciókba ossza a tranzakciók átfogó olvasatát a kezdetekig. A jelentősége a hatóságok számára a büntetőeljárásban az, hogy az összes tranzakció adatbázisaként funkcionál, s minden további intézkedés nélkül képes arra, hogy hiteles adatokat szolgáltatson.⁶⁸

Itt arról van szó, hogy ez egy elosztott információ, ami olyan elrendezési blokkokat tart fenn, amelyek egyrészt hamisításbiztosak, másrészt egyedi tranzakciókat tartalmaznak. A résztvevő csomópontok mindegyike egy teljes helyi másolatot őriz a blokkláncról. A blokklánc olyan blokk sorozatokból áll⁶⁹, amelyek a főkönyvek tranzakcióit tartalmazzák, ezek a tranzakciók időrendi sorrendben találhatóak meg, és minden blokk tartalmazza a láncon belüli előző blokk kriptográfiai kivonatát. A blokklánc négy olyan elemet tartalmaz, amit replikálni

⁶⁵ FRÖWIS, Michael – GOTTSCHALK, Thilo – HALSHOFER, Bernhard – RÜCKERT, Christian – PESCH, Paulina: Safeguarding the evidential value of forensic cryptocurrency investigations, In: *Forensic Science International: Digital Investigation*, 2020./33., 1. o. (<https://www.sciencedirect.com/science/article/pii/S1742287619302567>) utolsó megnyitás: 2024.10.11.)

⁶⁶ PESZLEG Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük, In: *Ügyészek Lapja*, 2010./2., 25. o. (https://www.ugyeszek.hu/ftp/tartalom/ugyeszek_lapja/2010/ul2010_2_all.pdf?phpMyAdmin=5e79130c4a2a408b3f002bed9c4d2fba) utolsó megnyitás: 2024.10.11.)

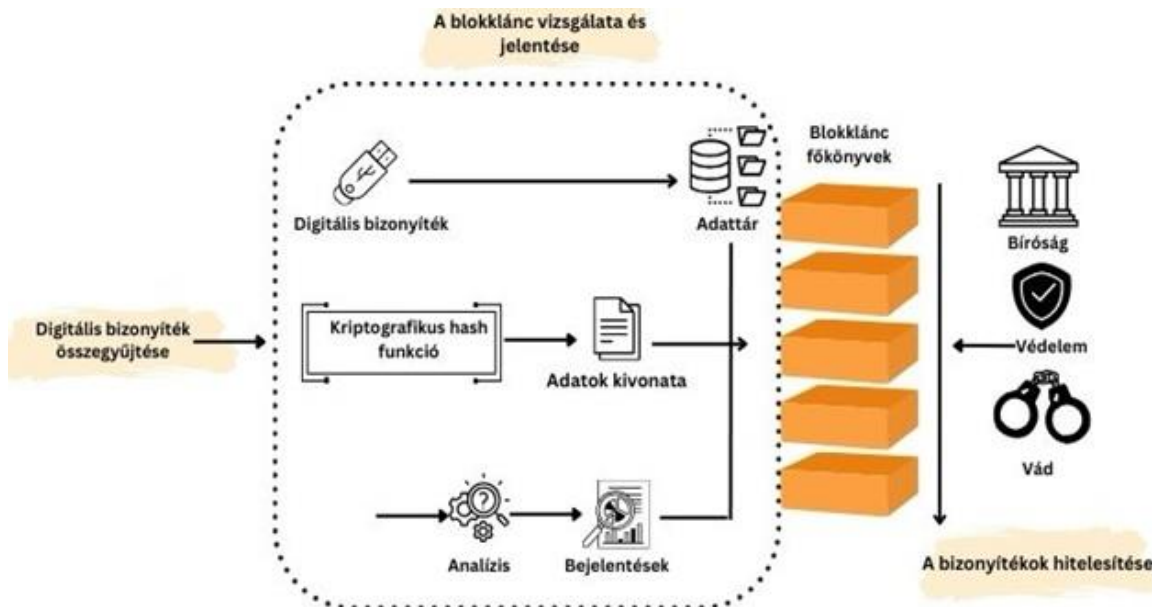
⁶⁷ 2017. évi XC. tv. Be. 205.§

⁶⁸ MISKOLCZI Barna – SZATHMÁRY Zoltán: *Büntetőjogi kérdések az információk korában*, Budapest, Orac Kiadó, 2018, 154-155. o.

⁶⁹ DUDANI, Sahil – BAGGILI, Ibrahim – REYMOND, David – MARCHANY, Randolph: The current state of cryptocurrency forensics, In: *Forensic Science International: Digital Investigation*. 2023./46., 2. o. (<https://www.sciencedirect.com/science/article/pii/S2666281723000859?via=ihub>) utolsó megnyitás: 2024.11.07.)

lehet, ezek az alábbiak: a főkönyv, a kriptográfia, konszenzus, s végül az üzleti logika. Ahogyan említettem, a blokkláncot a bizonyításhoz fel lehet használni, ebből a CoC (*felügyeleti lánc*)⁷⁰-t használják fel a bírósági eljárásokban, amelyről igazolni kell, hogy nem változott a nyomozás során, hiszen a bizonyítéknak úgy kell megérkeznie a bíróságra, mint amilyen formában először hozzájutottak.⁷¹

2. ábra: A blokklánci bizonyíték vizsgálata, és útja a bíróságra⁷²



1. A CoC, azaz a felügyeleti lánc – mint bizonyítási eszköz – bemutatása a Bitcoin tekintetében

A dolgozatomban azért foglalkozom kiemelten a Bitcoinnal, mivel ez a legszélesebb körben elterjedt kriptovaluta. Annak köszönhetően, hogy a Bitcoin már több, mint egy évtizede jelen van, rengeteg adat és tapasztalat gyűlt össze a használatáról és a biztonsági kihívásairól. Emiatt is mondható az el, hogy a Bitcoinhoz kapcsolódik a legtöbb csalás és visszaélés.

⁷⁰ CoC: Chain of Custody= felügyeleti lánc: ez egy olyan folyamat, amely nyomon követi a bizonyítékok mozgását a gyűjtésükön keresztül, s dokumentálja az összes olyan adatot, ami azt tartalmazza, hogy kik kezelték. AYERS, Rick – BROTHERS, Sam – JANSEN, Wayne: *Guidlines on Mobile Device Forensics*, Amerikai Egyesült Államok, U.S. Department of Commerce, 2014, 67. o.

⁷¹ GOPALAN, Harihara – SUBA S., Akila – ASHMITHASHREE, C. – GAYATHRI, A. – JEBIN ANDREWS, V.: Digital Forensics Using Blockchain: In: *IJRTE*. 2019./11. (https://www.researchgate.net/publication/362153704_Digital_Forensics_using_blockchain) utolsó megnyitás: 2024.10.22.)

⁷² SHIRAZI SYED, Atir Raza – TAHIRA, Khadija – SHAIKH, Mehwish: Cryptocurrency Investigation in Digital Forensics: Contemporary Challenges and Methodical Advance, In: *Acadlore*, 2023./2., 128. o. (https://www.researchgate.net/publication/373825791_Cryptocurrency_Investigations_in_Digital_Forensics_Contemporary_Challenges_and_Methodological_Advances) utolsó letöltés: 2024.10.19.)

A Bitcoin fellelésének legproduktívabb módja, ha sikerül azonosítani a privát kulcsokat az elkövetőnél. Annak érdekében, hogy a Bitcoin-hálózaton zajló titkosított, valamint anonim tranzakciókat megismerhessük, szükség van egy olyan módszerre, amelyek nyilvános adatbázisként működnek. Ez a módszer a blokklánc elemzés, amelyben rendkívül fontos szerepet játszik a felügyeleti lánc megismerése. Abban az esetben, ha sikeresen tártuk fel a blokkláncot, akkor megismerhetővé válik a láncolatban lévő személy nyilvános kulcsa, valamint ezáltal a hozzá kapcsolódó további személyek kiléte is.⁷³ A felügyeleti láncban nem csak az előzetes „tranzakciók” találhatóak meg, hanem minden esetleges módosítás, amelyet a megismerése alatt végrehajtottak benne. Ha egy esetleges módosítás történik a bizonyítékul szolgáló felügyeleti láncban, onnantól kezdve nem terjeszthetik a bíróság elé, mint bizonyíték (a változás miatt).

Így kijelenthetjük azt, hogy a modern digitális korban a kiberbűnözés aktivitásával a digitális bizonyítékok összetettsége kifejezetten megnehezíti a bizonyítási folyamatokat. Egyéb problémaként merülhet fel az is, hogy ezek a bizonyítékok időérzékenyek, így az időbélyegek rögzítése kulcsfontosságú lehet egy eljárásban.⁷⁴

2. A felügyeleti lánc fő követelményei, ahhoz, hogy a bizonyításban felhasználható legyen

I. Integritás: azért jelentős kérdés ez, hiszen hogyha a megszerzéstől számítva sérült, onnantól kezdve nem használható fel a bírósági eljárásban a bizonyíték. Az alkalmazott címadatok integritásának biztosítása érdekében elegendő a kriptovaluta kódját beírni (pl.: BTC), valamint rögzíteni a legfrissebb blokk hash-t a Chain of Custody azonosítójaként.⁷⁵

II. Nyomon követhetőség: a megszerzés időpontjától kezdve, a lehető legkorábbi időpontra kell visszaszármaztatni.

III. Ellenőrizhetőség: annak a módszernek, mellyel feltárták az adott felügyeleti láncot, teljes mértékben ellenőrizhetőnek kell lennie.

⁷³ LAKATOS Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. In: *Belügyi Szemle*, 2017./1., 37. o.

⁷⁴ TSAI FU, Ching: The Application of Blockchain of Custody in Criminal Investigation, Taiwan, Elsevier Kiadó, 2021, 2-3. o. (<https://www.sciencedirect.com/science/article/pii/S1877050921017853> utolsó megnyitás: 2024.11.03.)

⁷⁵ FRÖWIS, Michael – GOTTSCHALK, Thilo – HALSHOFER, Bernhard – RÜCKERT, Christian – PESCH, Paulina: Safeguarding the evidential value of forensic cryptocurrency investigations. In: *Forensic Science International: Digital Investigation*, 2020./33., 5. o. (<https://www.sciencedirect.com/science/article/pii/S1742287619302567> utolsó megnyitás: 2024.10.11.)

IV. A bizonyíték manipulálásának elkerülése: a bizonyítékot nem lehet kicserélni, hiszen, ha ezt elrontják nem tudnak egy olyan módszert kiépíteni, amely támogatja a felügyeleti láncsal kapcsolatos folyamatot.⁷⁶

Ha egyes bizonyítékok manipuláltak, az leginkább onnan vehető észre, hogy magát a bizonyítékot az adat feltöltője hitelesítette, de az aláírás az adat szolgáltatójánál van, aki képes az adatok integritását ellenőrizni. Továbbá a hash-ben látszódik, hogy módosítás történt, így, ha a változás az adat szolgáltató tudomására jut azt mindenképp jeleznie kell.⁷⁷

⁷⁶ GOPALAN, Harihara – SUBA S., Akila – ASHMITHASHREE, C. – GAYATHRI, A. – JEBIN ANDREWS, V.: Digital Forensics Using Blockchain. In: *IJRTE*. 2019./11. (https://www.researchgate.net/publication/362153704_Digital_Forensics_using_blockchain utolsó megnyitás: 2024.10.22.)

⁷⁷ LI, Meng – LAL, Chagan – CONTI, Mauro – HU, Donghui: LEChain: A blockchain-based lawful evidence management scheme for digital forensics, In: *FGCS*, 2021./115., 415. o. (<https://www.sciencedirect.com/science/article/abs/pii/S0167739X1933167X?via%3Dihub> utolsó megnyitás: 2024.11.03.)

X. A lefoglalás bemutatása az elektronikus adat esetén, különös tekintettel a Bitcoin kriptovalutára, avagy „Őrizz meg mindent, ne változtass semmin!”

3. ábra: A Bitcoin lefoglalásának egyszerűsített menete



Dolgozatomban lefoglalás bemutatása mellett döntöttem, hiszen a lefoglalás a bizonyítékok biztosításának primer módja.

A Be. 315. § (1) szakasza felsoroló jelleggel rögzíti az elektronikus adat lefoglalását, amelyben egyfajta fokozatosság is mutatkozik.⁷⁸ Ez történhet az elektronikus adatról másolat készítésével, az elektronikus adat áthelyezésével, az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével, lefoglalásával, vagy a jogszabályban meghatározott más módon.⁷⁹

A Be. 315. § (2) bekezdése rendelkezik arról, hogy a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezését megakadályozza⁸⁰, ugyanis ezzel egyfajta keretszabályt alakítanak ki az ún. virtuális vagyontárgyak biztosításának.⁸¹ Elmondható, hogy a büntetőeljárás jog ezen szabályozás megalkotásakor a magánjogi dogmatikát megkerülve kodifikálta a virtuális valuták lefoglalását, amellyel lényegében egyfajta jogi státuszt biztosított a jelenségnek.⁸²

Wang úgy vélekedik, hogy három alapvető kritériumot kell betartani a bizonyítékok beszerzésénél: az eredeti adat ne sérüljön vagy módosuljon, az eredetivel bizonyítható legyen az egyezés, valamint a bizonyíték elemzése ne változtassa meg azt.⁸³

Ha az előbb felsorolt kritériumok közül bármelyik bekövetkezik, abban az esetben az eljárásban nem tud bizonyítékként funkcionálni, így véleményem szerint kulcsfontosságú a lefoglalás módszere. A címben szereplő idézet mentén kell biztosítani e folyamatnál a későbbi beavatkozásokat, illetve elindítani azt a dokumentációs folyamatot, amely a felügyeleti lánc

⁷⁸ MEZEI Kitti: Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok, In: *Belügyi Szemle*, 2019./ 10. 28. o.

⁷⁹ 2017. évi XC. Be. 315.§ (1) bekezdése

⁸⁰ 2017. évi XC. Be. 315.§ (2) bekezdése

⁸¹ CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): *Büntetőeljárás jog I–II. – új Be. – Kommentár a gyakorlat számára*. HVG-ORAC, Budapest, 2018.

⁸² MISKOLCZI Barna – SZATHMÁRY Zoltán: *Büntetőjogi kérdések az információk korában*, Budapest, Orac Kiadó, 2018, 163-164. o.

⁸³ WANG SHIUH, Jeng: Measures of retaining digital evidence to prosecute computer based cyber-crimes. In: *Computer Standards and Interface*, 2007./2., 218. o.

(CoC) formájában végigvonul a bizonyítékok kezelésének teljes útján. Ezen felügyeleti láncban az is fellelhető, hogy mikor, hol, kinek a felügyeletében volt az említett bizonyíték, valamint az állapotában bekövetkezett változást is magában foglalja.⁸⁴ Ezen esetben természetesen egy kutatással összekötött lefoglalás értendő.

Fontosnak tartom, hogy bemutassam azt, hogy a jogosultnak sosincs fizikai birtokában a kriptovaluta egységeknél.⁸⁵

Nehézségnek számít a lefoglalás esetén az, hogy nem elegendő egy olyan adathordozó eszközre átmásolni a Bitcoin pénztárcát, amelyet ezt követően tesznek írásvédetté, mivel ezzel érdemleges lefoglalás nem történik meg. A hatóságnak javasolt saját számítógépen létrehozni egy pénztárcát a tárolás érdekében, de ezt mind olyan szoftver segítségével, amely a Bitcoin fogadására alkalmas és a teljes blokklánc ismeretével bír. Javasolt két számítógép használata ezen tranzakciók folyamán, hogy mindenképp kizárják az esetleges rosszindulatú vírusok jelenlétét.⁸⁶

Az a személy, aki saját címére fogadja a Bitcoint, tisztában lesz a küldő címmel, is, ha ismeri a saját címét. Tehát ellenőrizhető lesz, hogy pontosan honnan is érkezett a tranzakció. A Bitcoin-hálózat a rajta keresztül átáramló tranzakciókat az egész hálózaton szétküldi, így azok teljesen nyilvánosak lesznek.⁸⁷

A nyomozóhatóságok számára mindez azt jelenti, hogyha sikerül azonosítani egy adott bűncselekményhez tartozó Bitcoin címet, majd az innen induló tranzakciók nyomon követése során egy címhez fognak vezetni, így a cím használójának vizsgálata elengedhetetlen lesz a büntetőeljárás folyamán.

A bizonyíték megtalálását követően, a fizetésre használt elektronikus adat lefoglalását úgy lehet megvalósítani, hogy a Bitcoin azonosítása érdekében⁸⁸ létre kell hozni továbbá egy privát kulcsot, - amelyet el kell küldeni egy hatósági címre, hogy hozzáférjenek a privát kulcshoz – valamint egy publikus kulcsot is, amely egy címként működik. A privát kulcsok megismerésére a leginkább elfogadott módszer az, hogy a tárcát az elkövető által igénybe vett

⁸⁴ MÁTÉ István Zsolt: A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban, In: *Magyar Rendészet* 2014./2. 33. o. (<https://folyoirat.ludovika.hu/index.php/magyrend/article/download/3981/3247> utolsó megnyitás: 2024.11.07.)

⁸⁵ MEZEI Kitti: Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok, In: *Belügyi Szemle*, 2019./ 10., 31. o.

⁸⁶ GYARAKI Réka Eszter: A számítógépes bűnözés nyomozásának problémái. Doktori értekezés. Pécs, 2018. 117.o. (<https://pea.lib.pte.hu/handle/pea/23144> utolsó megnyitás: 2024.11.02.)

⁸⁷ ESZTERI Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések, In: *Infokommunikáció és jog*, 2017./1., 26. o. (<https://core.ac.uk/download/pdf/227037197.pdf> utolsó megnyitás: 2024.10.19.)

⁸⁸ JÁMBOR Gellért: A kriptovaluták megjelenése, elterjedése és a jelenséggel szemben lehetséges jogi válaszok, In: *Magyar Rendészet* 2023./4., 122. o.

programmal tárják fel. Így lesz megismerhető az elkövető által megalkotott címek és az azokon helyet foglaló összegek is.⁸⁹ A publikus kulcs megjelenik majd a blokkláncban, ugyanúgy, mint a végrehajtott tranzakció.⁹⁰ Ha az előbb levezetett folyamattal elkészülnek a lefoglalás folyamán, egy ellenőrzés követi az elvégzett munkát. Meg kell győződni a tranzakció sikerességéről.

A bizonyítás nehézségei

A Bitcoin vagy más egyéb azonos technológiára épülő virtuális valuták vagyonfelderítés során a nyomozóhatóság számára a legnagyobb nehézséget az okozza, hogy a Bitcoin tranzakciók pszeudoanonim tranzakciók, mint ahogy említettem ezek lényegében nyilvánosan nyomunkövethetőek, de a konkrét személyhez nem köthetőek.⁹¹ Ennek következtében a nyomozóhatóságnak egyéb módszerekhez kell folyamodnia, hogy pontosan meg tudják állapítani, hogy kinek a tulajdonában van az adott kriptovaluta.

Problémaként említendő a titkosítás kérdésköre is. Egyre gyakoribb szegmenést képezik a kiberbiztonságnak a különböző titkosítási megoldások a bűnelkövetők által alkalmazott módszerek. A klasszikus „kövesd a pénzt” módszer a kriptovaluták esetén nehezen kivitelezhető. Az elektronikus bizonyítékok biztosítását akadályozzák a könnyen hozzáférhető VPN-ek, valamint az anonimizáló szolgáltatások. Ezek a szolgáltatások alapvetően a magánszféra védelmét szolgálnák, de adott esetekben éppen a bűncselekmények elkövetésében is közrejátszanak.⁹² Ebből kifolyólag éreztem relevanciáját annak, hogy bemutassam a lefoglalást.

Továbbá jól látszik a kutatásomból, hogy a 21. század elejére a digitális világ valamennyi területen forradalmi változásokat hozott, ugyanakkor új kihívásokkal is szembe állította a társadalmat, különösen a bűnözés, bűnözés-megelőzés terén. Az internet világa kiváló lehetőséget biztosított a bűnözőknek, hogy határokon átnyúló módon, sok esetben az anonimitás teljességével kövessenek el bűncselekményeket. A hagyományos bűnüldözési módszerek és jogi keretek nem voltak elegendőek ezen meglehetősen új formák hatékony

⁸⁹ HALÁSZ Viktor: A bitcoin működése és lefoglalása a büntetőeljárásban, In: *Belügyi Szemle*, 2018./7-8., 138.-139. o.

⁹⁰ DOMOKOS Andrea: A magyar büntetőeljárás és a digitalizáció, In: *Miskolci Jogi Szemle* 2020./1., 70. o. (https://www.mjsz.uni-miskolc.hu/files/10803/2_tartalom.pdf utolsó megtekintés: 2024.11.19.)

⁹¹ MÁTYÁS Szabolcs – FRIGYER László – PRILENSZKY Géza: A virtuális fizetőeszközök szerepe és jelentősége a vagyonvisszaszerzés során, In: *Belügyi Szemle*, 2021./3., 423.o.

⁹² MISKOLCZI Barna – SZATHMÁRY Zoltán: *Büntetőjogi kérdések az információk korában*, Budapest, Orac Kiadó, 2018, 177-179. o.

kezelésére, így sürgetővé vált egy olyan megoldás kidolgozása, amelyben nemzetközi összefogásra volt szükség.

XI. Unió szintű jogforrások

1. Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

A 2013-as irányelvként hivatkozott direktíva célja az volt, hogy minimumszabályokat állapítson meg a bűncselekmények tényállására és a kapcsolódó szankciókra vonatkozóan, ezzel közelítve a tagállamok büntetőjogát az információs rendszerek elleni támadásokkal kapcsolatban. Az irányelvnek továbbá célja a tagállamok illetékes hatóságai, mint például a rendőrség vagy a bűnüldözési szakszolgálatok, valamint az Unió szakosított ügynökségei – Eurojust, az Europol, vagy éppen az ENISA- közötti együttműködés javítása.⁹³ A jogalkotó nagy hangsúlyt fektetett az egységes fogalommeghatározásra is. A büntetőjogi tényállások esetében, az irányelv az információs rendszerekhez való jogellenes hozzáférést, a rendszer érintő jogellenes beavatkozást, a jogellenes adatszerzést, továbbá az adatot érintő jogellenes beavatkozást nevesíti, s kihangsúlyozza, hogy a tagállamok kötelesek büntetni az alább felsorolt bűncselekmények felbujtását, kísérletét és a bűnsegélyt is.

Ez a direktíva kötelező érvényű elköteleződést is tartalmaz az információcserére vonatkozóan. A tagállamoknak kötelező létrehozniuk egy olyan operatív kapcsolattartó pontot, amely 24 órán keresztül elérhető.⁹⁴

2. Az Európai Parlament és a Tanács (EU) 2023/1543. rendelete

Az első és legfontosabb céljuk ezzel a rendelettel az volt, hogy az elektronikus bizonyítékok kezelését meghatározzák:

Jelentősséggel bírt, hogy olyan szabályokat fektessenek le, amely alapján a tagállami hatóság a büntetőeljárásban közlésre kötelező európai határozatot vagy megőrzése kötelező európai határozatot bocsáthat ki. Kiemelendő az is, hogy ez alapján a szolgáltatásokat kínáló szolgáltatók az adatok helyétől függetlenül kötelesek az elektronikus bizonyítékokat megőrizni, továbbá megőrizni.⁹⁵

⁹³ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (2013), (1) bekezdés (<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040>) utolsó megnyitás: 2024.09.30.)

⁹⁴ GÁSPÁR Zsolt: Régi és új tendenciák a kiberbűnözésben, Doktori értekezés., Pécs 2024, 30. o. (<https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/gaspar-zsolt/gaspar-zsolt-muhelyvita-ertekezes.pdf>) utolsó megnyitás: 2024. 11.01.)

⁹⁵ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2023/1543 Rendelete, 2023. 1.cikk (<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32023R1543>) utolsó megnyitás: 2024.10.31.)

Második helyen a közlésre kötelező (KKEHT) és megőrzésre kötelező európai határozatokat (MKEHT) emelném ki:

A rendelet szabályozza, hogy milyen esetekben és hogyan kell az elektronikus bizonyítékokat közzétenni, valamint megőrizni, biztosítva ezzel a jogi garanciákat és a megfelelő eljárásokat.⁹⁶ A közlésre kötelező európai határozatról KKEHT tanúsítvány, míg a megőrzésre kötelező európai határozatról pedig MKEHT tanúsítvány kézhezvételének időpontjában elektronikus formában tárolt adatok, tartalmi adatok, vagy forgalmi adatok.⁹⁷

A címzett a MKEHT esetében késedelem nélkül⁹⁸, a KKEHT esetében haladéktalanul⁹⁹ köteles a kért adatot megőrizni. Ha KKEHT tanúsítványt kell teljesíteni akkor értesíteni kell a végrehajtó hatóságot, s az értesítést követően, ha a hatóság 10 napon belül¹⁰⁰ egyetlen olyan megtagadási okot sem jelez, amely kizáró ok lehetne, akkor az adatok továbbíthatóak.

Az MKEHT esetében egy 60 napos¹⁰¹ megőrzési kötelezettséget írnak elő, s ezen időszak után a kötelezettség megszűnik, kivétel abban az esetben, ha a KKEHT kibocsátásra kerül.¹⁰²

Tehát összegezve, az EU 2023/1543 rendelete három kulcsfontosságú területet érint, tekintettel a digitális bizonyítékok kezelésére, amelyeknek szerepe egyre inkább fokozódik:

- Az elektronikus bizonyítékok kezelése és felhasználása a büntetőeljárások során
- A Közlésre kötelező európai határozatok a hatóságok közötti információcseréhez
- Megőrzésre kötelező európai határozatok az elektronikus adatokat illetően, hogy biztosítsák azok elérhetőségét a büntetőeljárás során.
-

3. A NIS és a NIS 2 IRÁNYELV

A NIS, azaz a (EU) 2016/1148 irányelv volt az első kiberbiztonsági célzatú intézkedés, amelyben melynek célja, hogy megalkossák az uniós szintű minimumszabályozást a kibervédelemben, továbbá az információbiztonság területén. A hálózati és információs rendszerek magas szintű biztonságának meglétét célozta meg az Európai Unión belül.¹⁰³ A NIS

⁹⁶ Uo. 3.cikk

⁹⁷ Uo. 3.cikk (9) bekezdés

⁹⁸ Uo. 11.cikk (1) bekezdés

⁹⁹ Uo.10.cikk (1) bekezdés

¹⁰⁰ Uo. 10.cikk (2) bekezdés

¹⁰¹ Uo. cikk (1) bekezdés

¹⁰² GÁSPÁR Zsolt: Régi és új tendenciák a kiberbűnözésben, Doktori értekezés., Pécs 2024, 32. o. (<https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/gaspar-zsolt/gaspar-zsolt-muhelyvita-ertekezes.pdf> utolsó megnyitás: 2024. 11.01.)

¹⁰³ SZÉNÁSI Imre: Kritikus rendszer elemek jellemzői, azok kijelölése, valamint azok védelme. In: Nemzetbiztonsági szemle, 2024./2., 24. o. (<https://folyoirat.ludovika.hu/index.php/nbsz/article/view/7432/5994> utolsó megnyitás: 2024.11.08.)

az Unión belül olyan együttműködési csoportot állított fel, amelynek célja stratégiai együttműködés, a hatékony kommunikáció, valamint a bizalom kialakítása.¹⁰⁴

Mindezek ellenére az irányelv felülvizsgálatában olyan mértékű hiányosságokat véltek felfedezni, amelyek miatt felmerülhetett az, hogy nem tudták a helyesnek vélt módon kezelni a jövőben felmerülő kibervédelmi kihívásokat.¹⁰⁵ A helyébe az EU 2022/2555 irányelv lépett, azaz a NIS2. Az irányelv korszerűsítette a jogi kereteket, annak érdekében, hogy jobban alkalmazkodjon a növekvő digitalizációhoz, illetve a változó kiberbiztonsági fenyegetésekhez, mindemellett a hatáskörét kiterjesztette új ágazatokra, szervezetekre, s tovább növelte az Unió egészének a kiberbiztonsági rezilienciáját.¹⁰⁶

A SIRIUS projekt

Az címben említett projekt az Europol, az Eurojust, valamint az Európai Igazságügyi Hálózat közös kezdeményezése. Alapvetően az elektronikus bizonyítékok határokon átvitelő hozzáférését hivatott előmozdítani.¹⁰⁷ A digitális büntető igazságszolgáltatásra tett javaslatban kifejezte az Eurojust elnöke, hogy a határokon átnyúló bűncselekmények bizonyítása akkor lehetséges, hogyha a digitalizációval lépést tudnak tartani az európai rendészeti szervek is. A program különösen az online szolgáltatóktól származó adatok megszerzésére összpontosít. A projekt főbb céljai közé tartozik az oktatás és a képzés, melyben lehetőség nyílik azon ismeretek elsajátítására, amelyek a hatékonyabb digitális bizonyíték kezelést elősegítik. Kiemelendő továbbá az is, hogy olyan eszközöket fejlesztenek ki és mutatnak be, amelyek megkönnyítik a nyomozásokat adatelemzések szempontjából. A SIRIUS projekthez jelenleg 25 ország csatlakozott, és 36 bűnüldöző egység fogott össze annak érdekében, hogy hatékonyabban kezeljék az online térben fellelhető digitális bizonyítékokat. A program sikerességéről éves beszámolókat tesznek közzé.¹⁰⁸

¹⁰⁴ KOVÁCS László: Kiberbiztonság stratégiai megközelítése, 2018, Budapest, 98. o. https://real-d.mtak.hu/1180/7/dc_1600_18_doktori_mu.pdf

¹⁰⁵ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022/2555 Irányelve (2022) (2) bekezdés (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32022L2555> utolsó megnyitás: 2024.11.10.)

¹⁰⁶ SZÉNÁSI Imre: Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme. In: *Nemzetbiztonsági szemle*, 2024/2., 24. o. (<https://folyoirat.ludovika.hu/index.php/nbsz/article/view/7432/5994> utolsó megnyitás: 2024.11.08.)

¹⁰⁷ DOMOKOS Andrea: A magyar büntetőeljárás és a digitalizáció, In: *Miskolci Jogi Szemle* 2020./1., 75. o. (https://www.mjsz.uni-miskolc.hu/files/10803/2_tartalom.pdf utolsó megtekintés: 2024.11.19.)

¹⁰⁸ EUROPOL (2024) *SIRIUS Project*. Europol. <https://www.europol.europa.eu/operations-services-innovation/sirius-project> utolsó megnyitás: 2024.11.12.)

XII. Nemzetközi kitekintés, avagy az Amerikai Egyesült Államok szabályozása, különös tekintettel Florida Állam szabályozására

Kutatásom során nemzetközi kitekintést keretei között ismertetem Florida állam kriptovaluta szabályozását. Nyomós érvként volt jelen az állam kiválasztásánál az a tény, hogy a 2023-ban kiadott IC3 *cryptocurrency fraud report* alapján Florida államban született a második legtöbb bejelentés a kriptovalutákkal elkövetett csalások terén (5,076). A veszteségek terén (390,222,375 USD) a vizsgált állam a harmadik helyen van.¹⁰⁹ Az említett 2023-as év volt az első olyan év, amikor éves *cryptocurrency fraud report* publikálódott. Az IC3 emellett, 2023-ban kiadott egy *internet crime report*-ot is, amelyben az alábbi módon említi meg a kriptovalutákkal elkövetett befektetési csalásokat.¹¹⁰

4. ábra: A befektetési csalások megoszlása



A fenti diagram is hatékonyan szemlélteti azt, hogy ebben a hároméves periódusban a kripto befektetési csalások milyen igencsak felzárkóztak a befektetési csalásokon belül.

A befektetési csalások 2021-ben 1,45 milliárd dollárról, 3,30 milliárd dollárra emelkedett, ami 127%-os növekedést mutat, majd 2023-ra, egy 38%-os emelkedés mutatható ki, amelynek a végeredménye egy 4,57 milliárd dolláros veszteség. A kriptovalutákkal elkövetett csalások száma elég nagy hányadát teszik ki a befektetési csalásoknak, hiszen 2021-ben még „csak” 907 millió dolláros veszteség volt észlelhető, míg 2022-ben ez 2,57 milliárd dollárra nőtt, amely egy 183-os növekedést jelöl, ezt követően 2023-ra már csak egy 53%-os növekedés volt felismerhető, 3,96 milliárd dollárra nőtt a veszteségek száma.

¹⁰⁹ FEDERAL BUREAU OF INVESTIGATION, Internet Crime Complaint Center (2024) 2023. IC3 Cryptocurrency Report 8-9. o. (https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf)

¹¹⁰ INTERNET CRIME COMPLAINT CENTER (IC3) (2024) IC3 Annual Report 2023. Federal Bureau of Investigation. 12. o. (https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf utolsó megnyitás: 2024.11.13.)

A Florida State v. Espinoza eset bemutatása

Floridában a kriptovaluták használata, s az ezzel elkövetett bűncselekmények igen szigorú törvényi szabályozás alá esnek. A Bitcoinnal történő pénzmosás elleni jogi elemzést, valamint vizsgálatot kizárólag a szövetségi bíróságok végezték. Azonban Pascal Reid és Michell Abner Espinoza letartóztatása után Florida lett az első állam, amely az állami jogszabályok alapján indított eljárást a Bitcoin felhasználókkal szemben.¹¹¹

Michell Espinoza ellen három vádpontot hoztak fel az eljárásban elsőfokon.

a.) Az állam azzal vádolta Espinozát, hogy törvénytelenül végezte a pénzküldői tevékenységét, hiszen nem jegyezte be magát a Florida állambeli nyilvántartásba, ezzel megsértve a FL. Stat. 560.125 § 2013-ban hatályos rendelkezéseit.

b.) – c.) A második és harmadik vádpontban pénzmosással vádolták, amely sértette FL. Stat. 896.101 § rendelkezéseit.¹¹²

A Floridai „*Third District Court of Appeal*” tévesen hozott döntést, amikor elutasította az első vádpontot. A második és harmadik vádpont esetében is ez volt a helyzet, hiszen akkor még semmilyen szabályozás nem volt érvényben a virtuális valutákról köztük a Bitcoinról. Az Egyesült Államok Kincstára (FATF)¹¹³ emiatt 2014-ben egy külön fogalmat dolgozott ki a virtuális valuták meghatározására, amelynek értelmében jelen virtuális valuta egy digitális értékképviselő, amellyel digitális térben folytatható kereskedelem, s olyan funkciókat lát el, mint például csereeszköz, valamint értéktárolóként, de nem rendelkezik törvényes fizetőeszköz státusszal.¹¹⁴ Az FATF továbbá meghatározta a Bitcoin fogalmát is, amelyben kimondta, hogy nincsen központi hatósága, és nem áll mögötte semmilyen kormányzat. Egyenlegeket tartalmaznak, amelyek Bitcoin címeikként léteznek és a tranzakciós naplóban találhatóak meg, az az a blokkláncban.

Espinoza beleegyzett, hogy Bitcoint fog pénzre cserélni, s több találkozón is részt vett Arias nyomozóval és a negyedik találkozást követően – amikor már 30.000 dollárt adott volna

¹¹¹ PECK M., Brandon: *The Value of Cryptocurrencies: How Bitcoin Fares in the Pockets of Federal and State Courts*. 26 U. Miami Bus. L. Rev., Miami, 2017. 199. o.

¹¹² *State v. Espinoza*, 3D16-1860 (Fla. 3d DCA 2019.), 2-11. o.

(<https://cases.justia.com/florida/third-district-court-of-appeal/2019-3d16-1860.pdf?ts=1553533771>) utolsó megnyitás: 2024.11.16.)

¹¹³ *State v. Espinoza*, 3D16-1860 (Fla. 3d DCA 2019.), 2-3. o.

(<https://cases.justia.com/florida/third-district-court-of-appeal/2019-3d16-1860.pdf?ts=1553533771>) utolsó megnyitás: 2024.11.16.)

¹¹⁴ FATF REPORT: Virtual Currencies, Key definitions and potential AML/CFT risks, (2014), 4. o. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf> utolsó megnyitás: 2024.11.07.)

át Espinozának Arias nyomozó – már nem vette át a hamisított pénzt (amely a titkos nyomozást finanszírozta), valamint ezt követően letartóztatták.¹¹⁵

Az indokolás első körben kimondta, hogy nem volt megállapítható a pénzmosás vádja, mivel a Bitcoin, mint virtuális valuta nem minősül „pénznek”, így nem volt besorolható az akkor hatályos FL. Stat. 560.103. §-ba¹¹⁶ – Espinoza is erre hivatkozott. Ezt követően törvényi bővítés történt, amely kifejezetten tiltotta a virtuális valutákkal történő pénzmosást.¹¹⁷ Az új szabályozás céljai közt szerepelt az, hogy a kriptovalutákat – pl.: Bitcoin, Ethereum – pénzügyi eszközként elismerjék.

2017 nyarán Rick Scott kormányzó aláírta az 1379.-es számú törvényjavaslatot (House Bill 1379.), amelyet válasznak szántak a *Florida State v. Espinoza* ügy elutasítása után. A törvény 2017. július 1-én lépett hatályba és kiterjesztette a FL. Stat. 896. 101 § (2) (j)-t, amely oly módon határozta meg a virtuális valuta¹¹⁸ fogalmát, hogy egy olyan digitális vagy elektronikus formátumban lévő csereeszköz, amely nem képezi sem az Egyesült Államok, sem bármelyik más ország valutáját.¹¹⁹

Továbbá válasz volt az is, hogy az FL. Stat 560.125 § (1)¹²⁰ kimondja, hogy a pénzügyi szolgáltatási tevékenységgel foglalkozó személy vagy szervezet ebben az államban, ha az érintett személynek nincs engedélye nem folytathat pénzügyi szolgáltatást. Kivéve, ha mentesül ezen engedélyszerzési kötelezettsége alól, e fejezet alapján. Ha egy olyan személy által megy végbe a tranzakció, aki nincs feljogosítva arra, hogy ennek lebonyolításában részt vehessen, akkor érvénytelen maga a folyamat, továbbá az illetéktelen személy nem lesz jogosult sem a tőke, kamat vagy bármilyen egyéb díj beszedésére, átvételére sem a megtartására a tranzakcióval kapcsolatban.¹²¹

¹¹⁵ *State v. Espinoza*, 3D16-1860 (Fla. 3d DCA 2019.), 6-9. o.

(<https://cases.justia.com/florida/third-district-court-of-appeal/2019-3d16-1860.pdf?ts=1553533771>) utolsó megnyitás: 2024.11.16.)

¹¹⁶ FL. STAT. 560.103 § (2023) Regulations of Trade, Commerce, Investments, and Solicitations (http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0560/Sections/0560.103.html) utolsó megnyitás: 2024.12.08)

¹¹⁷ WALES, Justin – KOHEN, Matthew – FIELDS, Carlton – BURT, Jorden: State regulations on virtual currency and blockchain technologies. 2017. (<https://casetext.com/analysis/state-regulations-on-virtual-currency-and-blockchain-technologies?sort=relevance&resultsNav=false&q=>) utolsó megnyitás: 2024.10.26.)

¹¹⁸ FL. STAT. 896.101 § (2023) Florida Money Laundering Act. (2) bekezdés (j) pont (<https://law.justia.com/codes/florida/title-xlvi/chapter-896/section-896-101/>) utolsó megnyitás: 2024.10.29.)

¹¹⁹ CASETEXT: (2024) State Regulation on Virtual Currency and Blockchain Technologies (<https://casetext.com/analysis/state-regulations-on-virtual-currency-and-blockchain-technologies-3>) utolsó megnyitás: 2024.10.26.)

¹²⁰ FL. STAT. 560.125 § (2023) Money Service Businesses (1) bekezdés (<https://www.flsenate.gov/laws/statutes/2021/560.125>) utolsó megnyitás: 2024.10.26.)

¹²¹ JASPERSE, Joseph: (2024) 50-Stat Review of Cryptocurrency and Blockchain Regulation. University of Pennsylvania – Florida State. (<https://stevenscenter.wharton.upenn.edu/publications-50-state-review/>) utolsó megnyitás: 2024.10.23.)

Végül 2022-ben Ron DeSantis kormányzó aláírta CS/HB 273-as törvényt, amelyben meghatározta a kriptovaluták szabályozását. Az FL. Stat. 560.103. (36) -ra hivatkozva teszik meg a fogalom ismertetését. A CS/HB 273. elfogadása előtt nem szerepeltek törvényi szinten hogyan kezeljék kriptovaluta tranzakciókat.¹²²

¹²² MONDAQ (2024) Florida Governor Signs Legislation Easing Cryptocurrency Regulation. (<https://www.mondaq.com/unitedstates/fin-tech/1194902/florida-governor-signs-legislation-easing-cryptocurrency-regulation> utolsó megnyitás: 2024.10.25.)

Elemzés

Az általam bemutatásra került jogesetben is jól látszik, hogy a digitális bizonyítéknak hatalmas jelentősége van egy eljárás során. Igaz, a bemutatott jogesetben a nyomozó is közrejátszott az ügy sikerességében, de a felhasznált kriptovaluta bizonyítási eszközként szolgált az ügy további részében.

Amerikai tekintetben megemlíteném, hogy külön törvény foglalkozik a bizonyítással, valamint a bizonyítékok kezelésével.

Az amerikai szabályozást a bizonyítékok körében a *Federal Rules of Evidence* tartalmazza, amely végső soron egy szövetségi szabályozás, s Florida állam is ezt implementálta rendszerébe a *Florida Rules of Evidence*-ben. A *Federal Rules of Evidence* szabályozásból kiemelem a „Rule 101.”-es pontot, amely így szól:

„Egy hivatkozás bármilyen írásos anyagra, vagy más hordozóra vonatkozik, beleértve az elektronikusan tárolt információt is”.¹²³

Ugyan utal a meghatározás az elektronikus formára, de nem fordul elő a digitális bizonyíték kifejezés a jogszabály szövegében. Azonban megfigyelhető, hogy magának az adatrögzítés mozzanatának van jelentősége.

Az említett jogszabályon kívül, rendelkezésünkre áll egy digitális bizonyítékokkal foglalkozó csoport, amely az SWGDE (*Scientific Working Group on Digital Evidence*). Fennállásuk óta évről-évre fejlesztik a digitális bizonyíték fogalmát. A csoport meghatározása szerint a digitális bizonyíték nem más, mint olyan bináris formában tárolt vagy továbbított információ, amely bizonyító erővel bír.¹²⁴

Ebből a meghatározásból kitűnik, hogy a szakértői definíció a bináris formában történő tárolásra helyezi a hangsúlyt.

¹²³ UNITED STATES COURTS. *Federal Rules of Evidence*, 2023, Rule 101. Scope, definitions (6) bekezdés

¹²⁴ MÁTÉ István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban, Doktori értekezés, Pécs, 2017, 91. o. (<https://pea.lib.pte.hu/bitstream/handle/pea/16947/mate-istvan-zsolt-tezis-hun-2017.pdf?sequence=2&isAllowed=y> utolsó megnyitás: 2024.11.02.)

XIII. Javaslat

Javaslataim alapvetően nem a büntetőeljárási törvényünkre irányulnak, hiszen az új Be. igyekezett pótolni a hiányosságokat, ugyanis a tárgyi bizonyítási eszközök mellett, az elektronikus adatot is említi, mint bizonyítási eszközt. A törvény indokolásából kitűnik, hogy azért is vezették be, mert a jogalkotó kifejezett céljának minősült egy olyan büntetőeljárás kialakítása, amely a jövő kihívásaira is képes választ adni. Ennek fényében a hangsúlyt inkább a működést elősegítő háttér hatékonyságára kívánom helyezni.

Annak érdekében, hogy a kriptovalutákkal elkövetett bűncselekményeket vissza lehessen szorítani, az általam feltárt és tanulmányozott hazai, és nemzetközi szakirodalom alapján szorgalmazom az alábbiakat.

1) A blokklánccal kapcsolatos nyomozás, valamint az esetleges kényszerintézkedés során csak olyan személy vegyen részt – természetesen a kötelező résztvevőkön kívül – aki biztosítani tudja ennek helyes kezelését, valamint feltárását. Javaslatom arra alapozom, ahogy a dolgozat több szegmensében is kiemeltem, hogyha ezek az adatok megsérülnek, vagy nem megfelelően vannak kezelve, felhasználhatatlanná válnak a büntetőeljárás folyamán.

2) Előző pontból kifolyólag javaslom, hogy olyan szakemberek járhassanak el – az előbb említett folyamatokban, akik valóban szakmailag megkérdőjelezhetetlen tudással rendelkeznek, ezért szorgalmazom az edukációs programokat. Úgy gondolom, hogyha frekvenciátaliban jutnak a legújabb információk birtokába a nyomozók és szakértők könnyebben lépést tarthatnak a gyors digitalizációs újításokkal. Ennek célja, hogy elkerüljük a bizonyítékok sérülését vagy jogilag felhasználhatatlanná válását. Ez kulcsfontosságú a büntetőeljárások eredményességének biztosítása érdekében. Az oktatással kapcsolatos véleményemet – természetesen más aspektusban – de fenntartom az eljárásban résztvevő egyéb személyek részére is.

3) Olyan blokklánc analitikai rendszerek fenntartását is javaslom, amelyek korszerűen tudják elemezni a blokkláncokat. Elérhetőségüket tekintve legyen biztosított az ezzel foglalkozó szakembereknek, hogy gyorsabban tudjanak egy-egy blokkláncot elemezni, s eljuttatni a helyes elemzést a bíróságra. Az eredmények gyorsabb bírósági felhasználása segítené az eljárások hatékonyságát.

XIV. Záró gondolatok

A kutatásom során felállított hipotéziseimet alátámasztom az általam feltárt primer, valamint szekunder források alapján. A tanulmányom során próbáltam egy átfogó képet nyújtani a kriptovalutákkal elkövetett bűncselekmények világszerte növekvő tendenciájáról.

Kiemelendő továbbá, hogy a kriptovalutával elkövetett bűncselekmények esetében a bizonyítás egyes kérdései sokkal nagyobb kihívás elé állítják a nyomozóhatóságot, mint egy hagyományos értelemben vett bizonyításban. Kutatásomban több ponton is említettem, hogyha az elektronikus adatot, mint digitális bizonyíték akarjuk felhasználni, különös tekintettel kell eljárni, hiszen sérülékeny adatokról beszélhetünk.

Álláspontom szerint nagyobb szakértelmet igényel egy blokklánc feltárása a szakértő általi feltárását, mint egy hagyományos fizikai térben megjelenő bizonyíték elemzése, mivel, ha a blokklánc sérül a szakértők vagy a nyomozóhatóság tulajdonában amíg annak feltárását végzik, akkor a bíróságon nem használható fel, mint bizonyíték. Ebből azt a következtetést vonom le, hogyha nem megfelelő, vagy nem naprakész tudású szakértők járnak el a digitális bizonyítékok elemzésénél a büntetőeljárás megghiúsulhat, így a sértettek nem részesülhetnek az igazságszolgáltatásban. Abban az esetben, hogyha ez az egyetlen bizonyíték amire támaszkodhatnak, márpedig a kibertérben elkövetett bűncselekmények ügyében folyó nyomozások esetén túlnyomórészt nem áll rendelkezésre más bizonyíték, csakis az elektronikus adatok.¹²⁵

Továbbá a primer jogforrások elsajátítását követően úgy gondolom, hogy a nemzetközi együttműködések mind hazai, Európai Unió, valamint amerikai szinten kell fejleszteni kell, mert lépést kell tartani a technológia fejlődésével.

¹²⁵ DORNFELD László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. In: *Belügyi Szemle* 2018./2., 118. o.

FORRÁS– ÉS IRODALOMJEGYZÉK

KÖNYVEK

- BELOVICS E. – BÉRCES V.: *Büntető eljárásjog*. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2023
- BÉRCES V.: *A büntetőeljárás reformja és a bizonyítás alapkérdései*. ELTE Eötvös Kiadó Kft., Budapest, 2021
- KIRÁLY T.: *Büntetőeljárás jog*. Osiris Kiadó., Budapest, 2023
- MISKOLCZI B. - SZATHMÁRY Z.: *Büntetőjogi kérdések az információ korában*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018
- CASEY E.: *Digital evidence and computer crime*, Elsevier kiadó, 2011. USA
- CZINE Á.: L. fejezet – A lefoglalás. In: Belegi József (szerk.): *Büntetőeljárás jog I–II.* – új Be. – Kommentár a gyakorlat számára. HVG-ORAC, Budapest, 2018

FOLYÓIRATOK

- BARTKÓ R. – SÁNTHA F.: A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre. In: *Military and Intelligence Cybersecurity reserach Paper*, 2023/2. (<https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC%20RP%202023-2%20-%20Bartkó%20Róbert-Sántha%20Ferenc%20-%20A%20kibertér%20műveletek%20büntetőjogi%20értelmezésének%20lehetőségei.pdf> utolsó megnyitás: 2024.12.03.)
- BÁCSKAI M.: A kriptovaluták büntetőjogi értelmezése a pénzmosás és a lopás tükrében. In: *Ügyészek Lapja*. 2024/1. 103-110. o. (<https://ugyeszeklapja.hu/?p=4534> utolsó megnyitás: 2024.10.01.)
- DOMOKOS A.: A magyar büntető eljárás és a digitalizáció. In: *Miskolci Jogi Szemle*, 2020/1., 65-76. o. (https://www.mjsz.uni-miskolc.hu/files/10803/2_tartalom.pdf utolsó megtekintés: 2024.11.19.)
- DORNFELD L.: A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az Eu-ban. In: *Infokommunikáció és jog*, 2017/2., 37-42. o.
- DORNFELD L.: A kibertérben elkövetett bűncselekmények összefüggésben alkalmazható kényszerintézkedések. In: *Belügyi Szemle*, 2018/2. 115-135. o.

DORNFELD L.: A kriptovaluták és az e-bizalom kapcsolata. In: *Magyar Rendészet*, 2021/4., 211-227. o.

DORNFELD L.: Az elektronikus bizonyítás szerzése aktuális kérdései. In: *Kriminológiai Közlemények*, 2021/4., 241-256. o.
(https://www.kriminologia.hu/files/kiadvany/2019/16_dornfeldl.pdf utolsó megnyitás: 2024.10.04.)

BODNÁR P. A.: A digitális bizonyítékok megjelenése a büntetőeljárásban - különös tekintettel a szakértő igénybevételére. In: *Büntetőjogi Szemle*, 2021/1, 19-29. o.

KIRÁLY P. B.: A blokklánc-technológia nemzetközi kereskedelmi jogi összefüggései. In: *Külgazdaság*, 2019/3-4., 19-31. o.

H.G. SUBA A. - ASHMITHASHRE C. - GAYATHRI A. - ANDREWS J.: Digital Forensics Using Blockchain. In: *IJRTE*, 2019/11.
(https://www.researchgate.net/publication/362153704_Digital_Forensics_using_blockchain utolsó megnyitás: 2024.10.22.)

DUDANI S. - BAGGLI I. - RAYMOND D. - MARCHANY R.: The current state of cryptocurrency. In: *Forensic Science International: Digital Investigation*, 2023/46.,
(<https://www.sciencedirect.com/science/article/pii/S2666281723000859?via=ihub> utolsó megnyitás: 2024.11.07.)

ESZTERI D.: Egy bitcoinnal elkövetett vagyon elleni bűncselekmény és ahhoz kapcsolódó egyes jogi kérdések. In: *Infokommunikáció és Jog*, 2017/1. 25-31. o.

FRÖWIS M. – GOTTSCHAL T. - HASLHOFFER B - RÜCKERT C. - PESCH P.: Safeguarding the evidential value of forensic cryptocurrency investigations. In: *Forensic Science International: Digital Investigation*, 2020/33.
(<https://www.sciencedirect.com/science/article/pii/S1742287619302567> utolsó megnyitás: 2024.10.11.)

GÁBOR T. – KISS G. D.: Bevezetés a kriptovaluták világába. In: *Gazdaság és pénzügy*, 2019/1., 31-65. o.

HALÁSZ V.: A bitcoin működése és lefoglalása a büntetőeljárásban. In: *Belügyi Szemle*, 2018/7.8., 117-146. o.

JÁMBOR G.: A kriptovaluták megjelenése, elterjedése és a jelenséggel szemben lehetséges jogi válaszlehetőségek. In: *Magyar Rendészet*, 2023/4, 115-135. o.

LAKATOS A. A.: Az informatikai bűncselekmények és a bitcoin. In: *Belügyi Szemle*, 2017/1. 24-44. o.

M. PECK B.: *The Value of Cryptocurrencies: How Bitcoin Fares in the Pockets of Federal and State Courts*. 2017/1.

MÁTÉ I. Zs.: A bizonyítékok kezelése. Az igazságügyi szakértő a büntetőeljárásban. In: *Magyar Rendészet*, 2014/ 2., 29-38. o.

MÁTYÁS S. – FRIGYER L. - PRILENSZKY G.: A virtuális fizetőeszközök szerepe és jelentősége a vagyonvisszaszerzés során. In: *Belügyi Szemle*, 2021/3. 417-430. o.

MEZEI K.: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban. In: *Pro Futuro*, 2019/1, 79-98. o. (<https://ojs.lib.unideb.hu/profuturo/article/view/3906/5176> utolsó megnyitás: 2024.09.15.)

MEZEI K.: Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok, In: *Belügyi Szemle*, 2019/10. 25-40. o.

NOVAK M. - GRIER J. - GONZALES D.: New approaches to digital evidence acquisition and analysis. In: *NIJ Journal*, 2019/1., 280. (<https://www.ojp.gov/pdffiles1/nij/250700.pdf> utolsó megnyitás: 2024.11.11.)

PESZLEG T.: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. In: *Ügyészek Lapja*, 2010/2., 23-32. o. (https://www.ugyeszek.hu/ftp/tartalom/ugyeszek_lapja/2010/ul2010_2_all.pdf?phpMyAdmin=5e79130c4a2a408b3f002bed9c4d2fba utolsó megnyitás: 2024.10.11.)

POLT P.: Digitális fejlődés és büntetőjog – akkor és most. In: *Belügyi Szemle*, 2022/11., 2389-2393. o. (<https://belugyiszemlejournal.org/index.php/belugyiszemle/article/view/1140/1141> utolsó megnyitás: 2024.12.01.)

RÓTH E.: Az elektronikus adat mint új bizonyítási eszköz megjelenése a büntetőeljárási törvényben. In: *Miskolci jogi szemle*, 2020/3. 165-174. o. (https://www.mjsz.unimiskolc.hu/files/13834/19_rotherika_tordelt.pdf utolsó megnyitás: 2024.10.04.)

SHIRAZI S. – SHAIKH M. - TAHIRA K.: Cryptocurrency Investigations in Digital Forensics: Contemporary Challenges and Methodological Advances. In: *ACADlore*, 2023/2., 126-134. o. (https://www.researchgate.net/publication/373825791_Cryptocurrency_Investigations_in_Digital_Forensics_Contemporary_Challenges_and_Methodological_Advances utolsó megnyitás: 2024.11.19.)

SIMON B.: A kriptovaluták és a kapcsolódó rendészeti kihívások. In: *A bűnügyi tudományok és az informatika* 169-186. o., Pécs, Magyarország: MTA Társadalomtudományi Kutatóközpont. (<https://jog.tk.hun->

ren.hu/uploads/files/09_buntetojog_informatika_SIMONB.pdf utolsó megnyitás:
2024.09.16.)

SORBÁN K.: A digitális bizonyíték a büntetőeljárásban. In: *Belügyi Szemle*, 2016/11. 81-96. o.

SZÉNÁSI I.: Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme. In: *Nemzetbiztonsági Szemle*, 2024/2., 18-37. o.
(<https://folyoirat.ludovika.hu/index.php/nbsz/article/view/7432/5994> utolsó megnyitás:
2024.11.08.)

TSAI F.-C.: The Application of Blockchain of Custody in Criminal Investigation Process. In: *Procedia Computer Science*, 2021/192, 2779-2788.
(<https://www.sciencedirect.com/science/article/pii/S1877050921017853> utolsó megnyitás:
2024.11.03.)

VARGA N.- BIRHER N. - KNOLL-CSETE E.: A kriptovaluta szabályozása-jogi kihívások és kockázatok. In: *Humán Innovációs Szemle*, 2024/1.
(<https://ojs.ppke.hu/hisz/article/view/1161/1217> utolsó megnyitás: 2024.09.14.)

WANG S.-J.: Measures of retaining digital evidence to prosecute computer based cyber-crime. In: *Computer Standards & Interfaces*, 2017/2, 216-223. o.

INTERNETES FORRÁSOK

AYERS R. – BROTHERS S. - JANSEN W.: Guidelines on Mobile Device Forensics. *NIST Special Publication* 800-101., 2024.
(<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf> utolsó megnyitás: 2024.10.27.)

ENISA. Electronic evidence - a basic guide for First Responders, 2014. (https://www.era-comm.eu/EPPO/kiosk/pdf/ENISA_2014.pdf Utolsó megnyitás: 2024.10.03.)

Európai Bizottság. *Cybercrime*., Migration and Home Affairs, 2024. (https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en?prefLang=hu&etrans=hu
Utolsó megnyitás: 2024.11.12.)

Európai Parlament és Tanács. Hozzáférhetőbb elektronikus bizonyítékok a bűnözés elleni fellépés érdekében. Szakpolitikák., 2024. (<https://www.consilium.europa.eu/hu/policies/e-evidence/timeline-e-evidence/> Utolsó megnyitás: 2024.10.15.)

Az Európai Unió Tanácsa. Az Európai Unió kiberbiztonsági stratégiája: A kiberbiztonság, mint a nemzetközi biztonság alapvető eleme., 2016.

(<https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf> utolsó megnyitás: 2024.10.25.)

Az Európai Tanács. Az Európai Tanács következtetései., 2017. (<https://www.consilium.europa.eu/media/23972/22-23-euco-final-conclusions-hu.pdf> utolsó megnyitás: 2024.10.25.)

Az Európai Unió Tanácsa. A kiberbiztonságról szóló következtetések., 2017. (<https://www.consilium.europa.eu/media/31666/st14435en17.pdf> utolsó megnyitás: 2024.10.15.)

Az Európai Unió Tanácsa. Az Európai Unió kiberbiztonsági stratégiája: A kiberbiztonság, mint a nemzetközi biztonság alapvető eleme., 2016. (<https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf> utolsó megnyitás: 2024.10.25.)

Europol. *About Europol*, European Cybercrime Centre, 2022. (<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> utolsó megnyitás: 2024.09.09.)

Europol. *SIRIUS Project*. SIRIUS Cross-Border Access To Electronic Evidence., 2024. (<https://www.europol.europa.eu/operations-services-innovation/sirius-project> utolsó megnyitás: 2024.11.12.)

Europol. *Internet Organised Crime Threat Assessment (IOCTA)*, Internet Organised Crime Threat Assessment, 2024. (<https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> utolsó megnyitás: 2024.10.09.)

FATF. *Virtual Currencies, Key Definitions and Potential AML/CFT Risks.*, 2014. (<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf> utolsó megnyitás: 2024.11.07)

Federal Bureau of Investigation (FBI). Digital Evidence Policy Guide, Part 01. Federal Bureau of Investigation., 2024. (<https://vault.fbi.gov/digital-evidence-policy-guide/digital-evidence-policy-guide-part-01-of-01/view> utolsó megnyitás: 2024.11.04.)

Federal Bureau of Investigation (FBI). FBI Ten most wanted fugitive. New York, Amerikai Egyesült Államok., 2024. (<https://www.fbi.gov/wanted/topten/ruja-ignatova/@@download.pdf> utolsó megnyitás: 2024.10.18.)

Federal Bureau of Investigation (FBI). IC3, Annual Report., 2024. (https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf utolsó megnyitás: 2024.10.13.)

Federal Bureau of Investigation (FBI). IC3, Cryptocurrency Fraud Report. 2024. (https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf utolsó megnyitás: 2024.10.18.)

JASPERSE J.: 50-State Review of Cryptocurrency and Blockchain Regulation, 2022. (<https://stevenscenter.wharton.upenn.edu/publications-50-state-review/> utolsó megnyitás: 2024.10.23.)

Magyar Nemzeti Bank (MNB). 2024. évi sajtóközlemények. Fokozott befektetői kockázattal járhatnak a kriptoeszközök, kriptotőzsdék., 2024. (<https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2024-evi-sajtokozlemenyek/fokozott-befektetoi-kockazattal-jarhatnak-a-kriptoeszkozok-kriptotozsdek> utolsó megnyitás: 2024.09.20.)

NAKAMOTO S.: *Annual national training seminar*. Bitcoin: A Peer-to-Peer Electronic Cash System., 2008. (https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf utolsó megnyitás: 2024.09.15)

STABILE D. – PRIOR K. - KRISHNA Dhruva: *Mondaq*. Florida Governor Signs Legislation Easing Cryptocurrency Regulation., 2022. (<https://www.mondaq.com/unitedstates/fin-tech/1194902/florida-governor-signs-legislation-easing-cryptocurrency-regulation> Utolsó megnyitás: 2024.10.25.)

WALES J. - KOHEN M. - FIELDS C. - BURT J.: *Casetext*. State Regulations On Virtual Currency And Blockchain Technologies., 2022. (<https://casetext.com/analysis/state-regulations-on-virtual-currency-and-blockchain-technologies-3> Utolsó megnyitás: 2024.10.26.)

U.S. Department of Homeland Security.: *Homeland Security Investigations*., Cybercrime., 2022. (<https://www.dhs.gov/hsi/investigate/cybercrime> Utolsó megnyitás: 2024.09.02.)

MAGYAR JOGFORRÁSOK

Magyarország Kormánya. (2013.03.22). *Nemzeti Jogszabálytár.*, 1139/2013. (III.21.) Kormány határozat. (<https://njt.hu/jogszabaly/2013-1139-30-22> Utolsó megnyitás: 2024.09.02.)

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről (<https://net.jogtar.hu/jogszabaly?docid=a0400079.tv> utolsó megnyitás: 2024.10.25.)

2017. évi XC. törvény 165.§ a-f)

2017. évi XC. törvény 205.§

2017. évi XC. törvény 315.§ (1) bekezdése

2017. évi XC. törvény 315.§ (2) bekezdése

2024. évi VII. törvény 2.§ (<https://njt.hu/jogszabaly/2024-7-00-00> utolsó megnyitás: 2024.09.30.)

EURÓPAI JOGFORRÁSOK

Európai Parlament és a Tanács. *Az Európai Unió Hivatalos Lapja.* Az Európai Parlament és a Tanács 2013/40/EU IRÁNYELVE az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról., 2023. (<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040> utolsó megnyitás: 2024.09.30.)

Európai Parlament és a Tanács. *Eur-Lex.* AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/858. RENDELETE., 2022. (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32022R0858> utolsó megnyitás: 2024.09.13.)

Európai Parlament és a Tanács. *Eur-Lex.* AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555. IRÁNYELVE. 2022. (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32022L2555> utolsó megnyitás: 2024.11.10.)

Európai Parlament és a Tanács. *Eur-Lex.* AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2023/1114. RENDELETE. 2023. (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A02023R1114-20240109> utolsó megnyitás: 2024.09.14.)

Európai Parlament és Tanács. *Eur-Lex.* forrás: Az Európai Parlament és a Tanács (EU) 2023/1543 RENDELETE. 2023. (<https://eur-lex.europa.eu/eli/reg/2023/1543/oj> utolsó megnyitás: 2024.10.31.)

AMERIKAI JOGFORRÁSOK

State of Florida. *JUSTIA US Law*. FL Stat 896.101 §, 2023. (<https://law.justia.com/codes/florida/title-xlvi/chapter-896/section-896-101/>Utolsó megnyitás: 2024.10.29.)

State of Florida. FL. STAT. 560.125 § Money Service Businesses, 2023. (<https://www.flsenate.gov/laws/statutes/2021/560.125> utolsó megnyitás: 2024.10.26.)

State of Florida. FL. STAT. 560.103. § Regulation of Trade, Commerce, Investments, and Solicitations, 2023. (http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0560/Sections/0560.103.html utolsó megnyitás: 2024.12.08.)

The Committee on The Judiciary House of Rep. Federal rules of evidence. 2023., Washinton D.C., Egyesült Amerikai Államok.

AMERIKAI JOGESET

The State of Florida vs. Michell Espinoza, 3D16-1860 (Third District Court of Appeal 2019.)(<https://cases.justia.com/florida/third-district-court-of-appeal/2019-3d16-1860.pdf?ts=1553533771> utolsó megnyitás: 2024.11.16.)

DOKTORI, VALAMINT MTA ÉRTEKEZÉSEK

GÁSPÁR Zs.: Régi és új tendenciák a kiberbűnözésben, Doktori értekezés, Pécs, 2024. (<https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/gaspar-zsolt/gaspar-zsolt-muhelyvita-ertekezes.pdf> utolsó megnyitás: 2024.11.01.)

GYARAKI R. E.:A számítógépes bűnözés nyomozásának problémái. Doktori értekezés Pécs,2019.(<https://pea.lib.pte.hu/handle/pea/23144> utolsó megnyitás: 2024.11.02.)

KOVÁCS L.: Kiberbiztonság stratégiai megközelítése, MTA Doktori értekezés, Budapest, 2018. (https://real-d.mtak.hu/1180/7/dc_1600_18_doktori_mu.pdf utolsó megnyitás: 2024.12.03.)

MÁTÉ I. Zs.: Az igazságügyi informatikai szakértő a büntetőeljárásban, Doktori értekezés, Pécs, 2017. (<https://pea.lib.pte.hu/bitstream/handle/pea/16947/mate-istvan-zsolt-tezis-hun-2017.pdf?sequence=2&isAllowed=y> utolsó megnyitás: 2024.11.02.)

TÁBLÁZAT, VALAMINT ÁBRAJEGYZÉK ¹²⁶

1. táblázat: Kriptovalutával elkövetett bűncselekmények bejelentéseinek megoszlása az USA-ban 14. o.
1. ábra: Kriptovalutával elkövetett bűncselekmények miatti pénzübeli veszteségek az USA-ban 14. o.
2. ábra: A blokklánci bizonyíték vizsgálata, s útja a bíróságra 22. o.
3. ábra: A Bitcoin lefoglalásának egyszerűsített menete 25. o.
4. ábra: A befektetési csalások megoszlása 32. o.

¹²⁶ A táblázat, továbbá az ábrák is saját fordításúak, valamint készítésűek.