DOI 10.26521/Profuturo/1/2019/3906

Mezei Kitti*

A kriptovaluták kihívásai a büntető anyagi és eljárási jogban[1]

kriptovaluták – Bitcoin – csalás – pénzmosás – virtuális pénztárca – lefoglalás

A *blockchain* technológia[2] megjelenésével párhuzamosan terjedt el a virtuális fizetési és értékképzési rendszerként működő *kriptovaluták* használata. A *bitcoin* 2009-es bevezetése óta a *kriptovaluták* témakörét különböző szakpolitikai döntéshozók vizsgálták eltérő megközelítést alkalmazva, azonban közös vonás, hogy valamennyien a virtuális fizetőeszközök egyik alcsoportjának sorolták be.[3]

Nem tekinthetők pénznek, mert a pénzkibocsátás intézmény által, szigorúan szabályozott keretek között történik, ezzel szemben a *kriptovaluták* nem rendelkeznek központi kibocsátóval, hanem komplex matematikai feladatokat megoldó számítógépek hálózatának segítségével jönnek létre. Fizikai formában nem, csak digitáli-

* Dr. Mezei Kitti tudományos segédmunkatárs, Társadalomtudományi Kutatóközpont Jogtudományi Intézet; doktorjelölt, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola; mezei.kitti@tk.mta.hu.

1 A tanulmány a 2018. november 5-én, a Pécsi Tudományegyetem Állam- és Jogtudományi Karán megrendezett *„Jogi és gazdasági kihívások a kriptovaluták világában”* című konferencián elhangzott előadás szerkesztett és továbbfejlesztett változata; az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

2 Az elosztott főkönyvi technológiának (*distributed ledger technology*, avagy DLT) a leggyakrabban előforduló formája a *blockchain* (blokklánc). A DLT a tulajdonjog nyilvántartására szolgál – legyen szó pénzeszköz vagy más eszköz, vagyonelem tulajdonjogáról. Jelenleg a bankok ügyleteiket – vagyis azon műveleteiket, amelyek keretében pénz- vagy egyéb pénzügyi eszközük tulajdonjoga gazdát cserél – centralizált rendszereken keresztül bonyolítják le, amelyeket gyakran központi bankok üzemeltetnek. Az elosztott főkönyv ezzel szemben olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják. A blokklánc esetén a tranzakciók csoportonként, azaz blokkonként időrendi sorrendben egymáshoz kapcsolva láncot alkotnak. A teljes láncot összetett matematikai algoritmusok védik, ezek gondoskodnak az adatok sértetlenségéről, biztonságáról. A lánc képezi az adatbázisban szereplő összes ügylet – mint például a tranzakciók – átfogó nyilvántartását, ami a hálózat minden tagja számára elérhető. Lásd az Európai Központi Bank honlapját (Eurorendszer, Kisokos) – Hogyan formálhatják át a technológiai újítások a pénzügyi piacokat? 2017. április 19. https://www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html (2019. 01. 04.).

3 *Virtual Currency Schemes.* Európai Központi Bank, Frankfurt, 2012, 13., https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (2019. 01. 04.). A Pénzügyi Akció Munkacsoport (Financial Action Task Force, FATF) ehhez hasonlóan átváltható és nem átváltható virtuális fizetőeszközöket különböztet meg. Virtual Currencies – Key definitions and Potential AML/CFT Risks. FATF, 2014, 4. Bővebben még erről: Houben, Robby–Snyers, Alexander: *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion.* Európai Parlament, Brüsszel, 2018. július, 20–22. PE 619.024. http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (2019. 02. 11.).

san érhetők el, de törvényes fizetőeszközre át- és visszaválthatók, valamint egyes *kriptovaluták* nem hozhatók létre végtelen mennyiségben.

A *kriptovaluták* rendszere decentralizált, vagyis közvetítő közbeiktatása nélkül működik, ami azt jelenti, hogy az utalásokat a felhasználók közvetlenül egymás között tudják lebonyolítani (*Peer-to-Peer* rendszer). Független, mert nem áll mögötte egyetlen ország, azok jegybankja vagy más szervezet sem, a működése a felhasználók közös megegyezésén, bizalmán alapul. Nincs mögötte aranyalap, valuta vagy egy állam gazdasága, a *kriptovaluta* értékét kizárólag a kereslet és a kínálat viszonya határozza meg. A *kriptovaluták* alapját – mint ahogy az elnevezésük is utal rá – a kriptográfia jelenti, ami egyszerűen fogalmazva, egy az információ védelmét biztosító technika, amely titkosítja, azaz olvashatatlan formátumra alakítja át azt, amit csak a titkosítást feloldó kulccsal rendelkező személy képes feloldani.

A *bitcoin* (BTC) az első *blockchain*-alapú *kriptovaluta*. A *bitcoin* lényegét tekintve egy generált számítástechnikai adat, amely tranzakciók feldolgozása és jóváhagyása révén keletkezik, egy előre meghatározott rendben, algoritmus alapján. Ezt a folyamatot nevezzük bányászásnak. Az így keletkező virtuális „érméket" a rendszer elosztja a „bányászok" között, akik a rendelkezésük alatt álló számítógépekkel támogatják és üzemeltetik a hálózatot. A létrehozható érmék száma korlátozott, maximum 21 millió *bitcoint* bányászhatnak ki. A rendszer lényege miatt az újabb érmék előállítása egyre nagyobb és nagyobb erőforrásokat igényel.[4]

A *Bitcoin* elnevezés egyben egy digitális fizetési rendszert is magában foglal, amelynek a kifejlesztése *Satoshi Nakamoto* nevéhez fűződik.[5] Kliensszoftvere ingyenes, nyílt forráskódú,[6] a *bitcoin* tranzakciók nyilvánosan nyomon követhetőek – a blokklánc működéséből adódóan –, vagyis rögzíti a feladó és címzett felekhez tartozó ún. *Bitcoin*-címeket és a tranzakciók összegét a blokkcsatornán, azonban ezek nem köthetők konkrét személyekhez.[7] Ezek ezért ún. *pszeudoanonim* tranzakciók.[8] Digitális javaknál felmerül egy probléma, ami a fizikai formában létező eszközöknél nem. Egy adott pénzérme vagy bankjegy fizikailag csak egyvalakinek a birtokában lehet, míg virtuális javakat korlátlan mennyiségben másolhatunk, így több, az eredetivel egyező másolatpéldány jöhet létre. Nyilvánvaló, hogy nem engedhető meg, hogy ugyanazt az érmét valaki több helyen is elköltse, illetve egynél több személy birtokolja. Ennek megoldására a *Bitcoin*-rendszerben a résztvevők csak azt a tranzakciót fogadják el érvényesként egy adott érme elköltésére, amelyik időben előbb következett be.[9]

[4] Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog,* 2015/11, 642.

[5] Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin White Paper Repository, 2008. https://bitcoin.org/bitcoin.pdf (2019. 01. 15.). A név valójában egy magát meg nem nevező programozót – vagy programozók csoportját – takar.

[6] A „nyílt forráskód" azt jelenti, hogy a technológia és a szoftver beépített, tesztelhető és a felhasználók együttműködésén keresztül fejlesztik.

[7] A https://blockchain.info/ oldalon a *bitcoin* – és már az *ether* – tranzakciók is nyomon követhetők.

[8] A *pszeudoanonimitás* azt jelenti, hogy *„van alanya az adatoknak, de az alany valós kilétét nem ismerjük; egy valós adatalanynak több fedőneve, profilja, virtuális személyisége is lehet".* Az anonimitás lényege, hogy *„az adatokat, illetve az adatok kezelésével járó eseményeket, cselekvéseket nem tudjuk egy meghatározott személylyel kapcsolatba hozni".* Székely Iván: Privát szférát erősítő technológiák. *Információs Társadalom,* 2008/1, 25.

[9] Tüzes Marcell: Bitcoin – A pénz új formája. *Infokommunikáció és Jog,* 2012/4, 156.

Az utaláshoz egy kulcspár szükséges, amely egy nyilvános kulcsból *(public key)* – ez más néven a *Bitcoin*-cím,[10] ami hasonló a bankszámlacímhez és mindenki számára nyilvános –, valamint egy privát kulcsból *(private key)* áll,[11] ami pedig jelszóként funkcionál, és csak az adott felhasználó számára elérhető. A privát kulcs ismerete szükséges ahhoz, hogy az adott címhez kapcsolt *bitcoin*-egységeink felett rendelkezhessünk, és utalásokat végezzünk. A privát kulcsból kinyerhető a nyilvános kulcs, míg fordítva erre nincs lehetőség. A kulcspár segítségével utalhatunk a kliensprogramon keresztül, amely ún. virtuális pénztárca *(wallet)* is egyben, és amelynek a fő funkciója a privát kulcs létrehozatala és tárolása. A *kriptovaluta* tárcánk nem más, mint egy fájl a számítógépen, amelyet *wallet.dat* néven találhatunk meg.[12] Ennek védelme érdekében számos intézkedés tehető, így például a fájl titkosítható, biztonsági másolat készíthető róla, vagy akár *online,* jelszóval ellátott tárhelyen tárolható, akár a felhőben.[13] Különböző *kriptovaluta*-tárca típusok használhatók, amelyek között vannak az internetre valamilyen formában csatlakozó ún. „forró tárcák" *(hot wallet):*

– Asztali vagy mobiltárca: a privát kulcsot a számítógépen *(Jaxx)* vagy a mobiltelefonon tárolják.
– Web-alapú pénztárca: egy szolgáltató online felületén érhető el *(Coinbase),* azonban ebben az esetben nem mi rendelkezünk a privát kulcsunkkal, és ez kockázatos, mert a pénztárca-szolgáltatók gyakran célpontjaivá válnak a kibertámadásoknak, és további visszaélésekre adnak lehetőséget.

A másik típus az ún. „hideg" vagy *offline* tárolás, amely a legbiztonságosabb megoldást nyújtja:

– Hardveres pénztárca: hardverkulcs alkalmazását jelenti, amely egy speciális pendrive-hoz hasonló eszköz, a hardverbe épített elektronika tárolja a privát kulcsot *(Ledger Wallet, Trezor).*
– Papíralapú tárca: a kulcspár papírra történő kinyomtatását jelenti (például QR-kódként).
– Agypénztárca *(brain wallet):* amikor a felhasználó megjegyzi a privát kulcsot.[14]

Érdemes ismertetni a *kriptovaluták* piacán jelen lévő kulcsszereplőket is.

– Felhasználók: a *kriptovalutával* rendelkező természetes vagy jogi személyek.
– Bányászok: a tranzakciók jóváhagyásában vesznek részt – amihez a hálózatban részt vevők 51%-ára van szükség –, és ezért cserébe a kibányászott *kriptovalutából* meghatározott egységet kapnak, valamint csekély tranzakciós díjban részesülnek.
– *Kriptovaluta* tőzsdék és átváltók *(cryptocurrency exchanger;* például *Coinbase, Kraken, Binance, Bitfinex):* a felhasználók számára különböző szolgáltatásokat

[10] 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55.
[11] 5JBvhsfA5JesmcVTGNrb3gkHGgv67hwY5hUws1Pmdj65jRM9nPF.
[12] Eszteri Dániel: Bitcoin – Az anarchisták pénze vagy a jövő fizetőeszköze? *Infokommunikáció és Jog,* 2012/2, 71.
[13] Szathmáry (2015): i. m., 642–643.
[14] Simon Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* PTE ÁJK–MTA TK, Budapest–Pécs, 2019, 175.

nyújthatnak, így – a hagyományos tőzsdékhez hasonló módon – a *kriptovaluták* eladását és vételét meghatározott árfolyam alapján,[15] és/vagy a *kriptovaluták fiat* (rendeleti) pénzre vagy másik *kriptovalutára* történő átválását, meghatározott díj ellenében (átváltó-szolgáltató). Emellett a pénztárca-szolgáltatóknak megfelelő funkciókkal is rendelkezhetnek. A szolgáltatások típusai szolgáltatónként eltérhetnek. Általában minden *kriptotőzsde* egyben átváltó is, azonban nem minden átváltó *kriptotőzsde.*

– Kereskedési platformok: színteret biztosítanak a felhasználók számára, hogy egymás között bonyolítsák le a *kriptovaluta* adásvételüket *(LocalBitcoins).*
– Letétkezelő pénztárca-szolgáltatók: a felhasználók virtuális pénztárcáinak, a kulcspároknak nyújtanak online tárolási lehetőséget.[16]

A *bitcoinon* kívül érdemes az egyéb *kriptovalutákról,* ún. *altcoinokról*[17] is említést tenni, amelyek más előnyös tulajdonságokkal rendelkeznek, és ezért egyre többen használják ezeket; ilyen például az *ether,* a *Dash,* a *Zcash* és a *Monero.*

Az *Ethereum (ETH)* egy decentralizált platform, amely okosszerződéseket[18] futtat, éppen ezért az alkalmazásában sokkal nagyobb lehetőség rejlik. Ebben az esetben az *ether* a *kriptovaluta.* Ennek kínálata növekszik, és évente kerül korlátozásra. A *kriptovaluta* kereskedésen kívül az *ethert* a fejlesztők is használják, az *Ethereum* hálózaton történő szolgáltatások kifizetéséhez. Az *Ethereum* gyorsabb tranzakciókat biztosít: a *bitcoin* esetén 10 perc egy utalás, míg az *Ethereum* használatakor 14 másodperc.[19]

A *Dash (DASH)* szintén bányászható és nyílt forráskódú *kriptovaluta*. A *bitcoinhoz* képest gyorsabban, 4 másodperc alatt végzik az utalásokat. Emellett lehetővé teszik a privát védelmet a blokkcsatornán, különösen a *PrivateSend* funkció választásával, ami az ún. *coin-mixing* szolgáltatás használatával történik, így a tranzakció során az adott felhasználó által küldött összeget összekeverik más felhasználókéval annak érdekében, hogy ne lehessen visszakövetni annak eredeti forrását.[20]

A *Zcash (ZEC)* szintén egy decentralizált és nyílt forráskódú kriptovaluta, amely azonban már a teljesen nyílt tranzakció-történetet biztosító típusokkal ellentétben lehetőséget ad a részt vevő feleknek arra, hogy a pénzügyi műveletek részleteit titkosítsák. A tranzakciókkal kapcsolatos információk a *Zcash* esetén is nyilvánosan

[15] Tüzes: i. m., 157.

[16] Houben–Snyers: i. m., 25–27.

[17] Az Altcoinokon belül vannak, amelyek a Bitcoin nyílt forráskódját használják (Litecoin), és vannak, amelyek a saját forráskódjukat és elosztott főkönyvüket (Ethereum és a Ripple).

[18] Az okosszerződés egy olyan számítógépes protokoll, melyben egy digitális szerződés előre meghatározott feltételekkel teszi lehetővé a szerződő felek között a tranzakció megvalósulását. A szerződésben rögzített feltételek végrehajtásához nincs szükség harmadik félre. Kölvart, Merit–Poola, Margus–Rull, Addi: Smart Contracts. In: Kerikmäe, Tanel–Rull, Addi (eds.): *The Future of Law and eTechnologies*. Springer, 2016, 133–145. (https://doi.org/10.1007/978-3-319-26896-5_7); valamint Mik, Eliza: Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology,* 2017/2, 4–6. (https://doi.org/10.1080/17579961.2017.1378468).

[19] Girasa, Rosario: *Regulation of Cryptocurrencies and Blockchain Technology: National and International Perspectives*. Palgrave Macmillan, 2018, 39–40. (https://doi.org/10.1007/978-3-319-78509-7).

[20] Houben–Snyers: i. m., 48–49.

hozzáférhetők a blokkcsatornán, de a feladók és a címzettek azonosítója, valamint a tranzakciók összege rejtve maradhat. A kétféle cím – egy nyilvános cím és egy privát cím – közül maguk a felhasználók választhatnak, attól függően, hogy el kívánják-e rejteni a tranzakciós adatokat, vagy sem.

A *Monero (XMR)* ennél is nagyobb adatvédelmi biztonságot kínál, mivel beépített funkcióként az összes tranzakció teljesen rejtve van a *kriptográfia* mögött, ami egyaránt titkosítja a feladó és címzett feleket, valamint az átutalt összegeket.[21]

Mindezek alapján megállapítható, hogy egyes *kriptovaluták* a *bitcoinhoz* képest is magasabb fokú titkosítást képesek biztosítani, és a technológiai korlátok miatt potenciálisan lehetetlenné válik egy-egy tranzakció mögött álló személy azonosítása, valamint az illegális értékmozgás nyomon követése, ami növelheti a bűnelkövetési célú felhasználást.

Az elmúlt években a *bitcoin* piaci részesedése a *kriptovaluták* között csökkent (2015-ben 80%, míg 2017-ben 35%), azonban még mindig első helyen szerepel a bűnelkövetők által használtak között.[22]

A legnagyobb kihívást a *kriptovalutákkal* elkövetett bűncselekmények felderítésében az jelenti, hogy a tranzakciók nem köthetők konkrét személyekhez, mert ezen utalásokhoz nincs szükség személyazonosításra vagy hitelesítésre.

A decentralizáltságnak köszönhetően a virtuális fizetési rendszerek nem rendelkeznek központi felügyeleti szervvel, vagyis a büntetőeljárás során az eljáró hatóságok nem tudnak kihez fordulni a szükséges információkért, mint például a pénzintézetek esetén, amikor egyszerű banki megkeresés révén a pénzmozgás könnyen és egyszerűen nyomon követhető, valamint a pénzt küldő és fogadó személyek kiléte kideríthető.

Problematikus, hogy a virtuális fizetőeszközöknek nincs egységes szabályozásuk, ezért jelenleg jogilag „szürke zónába" esnek. Vannak ugyanakkor államok, amelyek már állást foglaltak a *kriptovalutákkal* kapcsolatban. Az egyik legprogresszívebb szabályozással Japán rendelkezik, mert a *kriptovalutákat* fizetőeszközként fogadja el, továbbá a *kriptovaluta* átváltó szolgáltatók tevékenysége is részletesen szabályozott. Működésük regisztrációhoz kötött és szigorú követelményeknek kell megfelelniük kiberbiztonsági szempontból, valamint a pénzmosás és a terrorizmus finanszírozása megelőzésének érdekében.[23] Németországban a pénzügyminisztérium állásfoglalása alapján „elszámolási egységnek" minősülnek, és szabadon lehet kereskedni velük. Az Egyesült Államokban szövetségi és tagállami szinten kerültek szabályozásra, azonban a különböző szabályozó szervek eltérően értékelik a jogi besorolásukat.[24]

A központi bankok általában egységes állásfoglalásokat fogalmaztak meg e kérdésben; így például az Európai Központi Bank és a Magyar Nemzeti Bank is közleményeket tett közzé, amelyekben felhívják a figyelmet arra, hogy a virtuális fizetőeszközök nem minősülnek törvényes fizetőeszköznek, illetve pénznek sem. Véleményük

[21] Houben–Snyers: i. m., 45–46.

[22] Europol (2018): i. m., 58.

[23] A módosított Payment Services Act No. 59. of 2009.

[24] Blemus, Stéphane: Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide. *Revue Trimestrielle de Droit Financier,* 2017/4, 1–15. (https://doi.org/10.2139/ssrn.3080639).

szerint a fizetésre alkalmas virtuális eszköz elnevezés lenne a helyes. Figyelmeztetnek, hogy ezen eszközök esetében hiányoznak a megfelelő felelősségi, garanciális és kárviselési szabályok is, amelyek például visszaélés, ellopás esetén védenék a fogyasztók érdekeit.[25]

Érdemes megemlíteni, hogy a hazai szakirodalomban *Eszteri Dániel* és *Szathmáry Zoltán* már részletesen vizsgálták a virtuális fizetőeszközök jogi státuszát a nemzeti jogban, és megállapították, hogy azok nem tekinthetők pénznek, értékpapírnak, vagyoni értékű jognak, árucikknek, valamint szellemi terméknek.[26] *Eszteri* szerint a *Bitcoin*-mennyiség feletti rendelkezési jogosultság a felhasználó vagyoni értékű jogának csak akkor tekinthető, ha az adott *bitcoin*-mennyiség egy konkrét szerződéses viszonyban jelenik meg. Azonban a *bitcoin* puszta létét a jelenlegi jogszabályi környezet nem tudja kezelni.[27]

1. A kriptovaluták bűnelkövetési célú felhasználása

Az *Europol* az évente közzétett, a szervezett bűnözés általi internetes fenyegetettséget vizsgáló jelentésekben[28] felhívja a figyelmet a *kriptovaluták* bűnelkövetési célú felhasználására, és rámutat arra, hogy az átlépett egy olyan értéket, ami miatt a rendvédelmi szervek fokozott figyelme szükséges.

A virtuális fizetőeszközökkel összefüggő bejelentések száma emelkedést mutat Magyarországon is. 2017-ben, a Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda összesen 38, virtuális fizetőeszközökkel kapcsolatba hozható bejelentést kapott, ezenfelül 3 tájékoztatást és 1 megkeresést fogadott külföldi pénzügyi információs egységektől. A bejelentések kétharmadában jellemzően megjelennek az ismertebb virtuálisfizetőeszköz-váltó platformok. 2017-ben 4 esetben került sor információtovábbításra, amelyek címzettje 3 esetben valamely rendőrségi szerv, 1 esetben a Terrorelhárítási Központ volt.[29]

A következő részben részletesen elemzem a *kriptovalutákkal* összefüggő egyes bűncselekményeket, a hazai és uniós szabályozásra tekintettel.

1.1. Csalás

A *kriptovaluták* megvásárlására általában vagy egy másik ilyen eszközzel rendelkező felhasználótól, vagy egy erre szakosodott tőzsdén keresztül van lehetőség.

[25] https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2016-evi-sajtokozlemenyek/fokozott-kockazatot-hordoznak-a-vilaghalon-elerheto-virtualis-fizetoeszkozok (2019. 01. 28.).

[26] Lásd Eszteri (2012): i. m., 71–78.; valamint Szathmáry (2015): i. m., 643–644.

[27] Eszteri Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. *Infokommunikáció és Jog,* 2017/1, 30.

[28] A legutóbbi jelentés: Internet Organised Crime Threat Assessment (IOCTA) 2019, Europol, 2019. 10. 09. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (2019. 10. 10.).

[29] Éves jelentés – 2017. év. Nemzeti Adó- és Vámhivatal Központi Irányítása Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda, Budapest, é. n., 11.

Ezt kihasználva jelent meg az a csalási módszer, hogy az elkövetők *bitcoin* értékesítését ígérik a sértetteknek, azonban a megbízásokat végül nem teljesítik. A nyomozó hatóságok erre következtetnek abból, ha a banki ügyfelek fizetési számláira jóváírások érkeznek, amelyek közleményei virtuális fizetőeszköz-kereskedelemre utalnak, azonban ezt követően a fizetési számlán csalás jellegű tevékenység miatt az átutalások törlését és az összegek visszautalását kérik.[30]

Érdemes említést tenni egy hazai esetről, amelyről *Eszteri* írt részletesen.[31] A konkrét eset történeti tényállása a következő: a sértett és az I. rendű vádlott e-mail üzenetváltás útján megállapodott abban, hogy a sértett a tulajdonában lévő 15 egységnyi *bitcoint* eladja I. rendű vádlott részére, aki ennek ellenértékét, összesen 2,5 millió forintot a *bitcoin* átutalását követően készpénzben fogja kifizetni. I. és II. rendű vádlott a megbeszélt helyen találkoztak a sértettel, aki magával hozta a laptopját, amit használva a vádlottak előtt átutalt 15 egységnyi *bitcoint* az elsőrendű vádlott által megadott címre. A sikeres átutalást követően II. rendű vádlott azt állította, hogy az átutalt *bitcoin*-mennyiség ellenértékeként ígért készpénz a parkolóban leállított gépjárműben található, ezért a sértett a vádlottak kíséretében elindult a parkolóba. A vádlottak a sértett előtt haladtak, majd miután kiléptek az áruház kapuján, hirtelen egymásra nézve és ezzel egymásnak jelt adva a személygépkocsihoz futottak, amibe mindketten beszálltak, majd az ajtókat belülről magukra zárták. A sértett a vádlottak távozását úgy akarta megakadályozni, hogy a személygépkocsi elé állt és abba kapaszkodott, amikor elindultak a gépjárművel. A kiérkező rendőrök a vádlottakkal szemben intézkedést foganatosítottak, őket igazoltatták. Először mindössze közúti veszélyeztetés és súlyos testi sértés kísérlete miatt, később a sértett vallomása alapján azonban már csalással gyanúsították meg a vádlottakat. Az ügy megítélése szempontjából fontos, hogy a vádlottakat először igazoltató járőrök láthatóan nem voltak tisztában az elkövetett bűncselekmény súlyával és helyes minősítésével, a vagyon elleni elemet meg sem említették a jelentésben. Ennek megfelelően a sértett kérése ellenére a vádlottak informatikai eszközeit sem foglalták le a helyszínen. Az ügyészség a vádlottakat a Btk. 373. § (1) bekezdésébe ütköző és (3) bekezdés *a)* pontja szerint minősülő nagyobb kárt okozó csalás bűntettének elkövetésével vádolta meg, mint társtetteseket. A vádlottak a sértettet szándékegységben cselekedve jogtalan haszonszerzés végett tévedésbe ejtették, mert a kialkudott vételár nem is állt a rendelkezésükre, és annak átadása nem is állt szándékukban. A bűncselekmény elkövetésével 2,5 millió forint kárt okoztak a sértettnek, ami nem térült meg. A sértett az ügy kapcsán polgári jogi igényt terjesztett elő. A járásbíróság is először csak a közlekedési és testi épség elleni elemet vizsgálta, a *bitcoin* mint pénzben kifejezhető ellenértékkel bíró virtuális vagyonelem értékelésétől pedig kezdetben elzárkózott.[32]

Ezen kívül érdemes felhívni a figyelmet a kriptovaluták világán belül az egyre népszerűbb és önálló területet felölelő elsődleges érmekibocsátásra, avagy az *Initial Coin Offering*-re (a továbbiakban: ICO). *„Az elsődleges érmekibocsátás az a folya-*

[30] Lásd ugyanott.

[31] Eszteri (2017): i. m., 25–31.

[32] Eszteri (2017): i. m., 25–26.

mat, amelynek során az új kriptopénzt első alkalommal kínálják eladásra az alkotók. Fiat vagy valamely vezető kriptopénz (általában *bitcoin és ether*) *ellenében vásárolhatunk belőle. Az árusítás azelőtt indul, hogy a kriptopénz* bármely *kriptotőzsdén vagy bármely váltó kínálatában megjelenne."*[33] Ez egy nyilvános forrásgyűjtési módot jelent, valamely ötlet vagy vállalkozás finanszírozásához, egy blokklánchálózat támogatásán keresztül. Ennek során az ötletgazda ún. *coint* (önálló, saját blokklánccal rendelkező *kriptovalutát*) vagy *tokent* (más által létrehozott platformon alapuló *kriptovalutát*)[34] bocsát ki, és kínál eladásra a támogatók részére hivatalos fizetőeszközért, vagy gyakrabban *kriptovalutáért* cserébe, így az ötletgazda, vagyis az ICO kibocsátója az eladott *kriptovalutákból* szerez pénzt az ötlet megvalósításához. Ezek a kriptoeszközök megtestesíthetnek egy jövőbeni áru vagy szolgáltatás igénybevételére vonatkozó jogosultságot is, az esetek többségében azonban nem mutatható ki megtestesített érték. Gyakoriak a visszaélések, ugyanis sok esetben az ICO-val összegyűjtött pénzből nem kezdik el megvalósítani a kitűzött célt, sőt ez nem is állt szándékukban, ezáltal a csalás tényállását valósítják meg.[35] Éppen ezért a jegybankok többsége is figyelmeztet, hogy ezek rendkívül kockázatos és spekulatív befektetési formának számítanak. 2018 elején pedig a visszaélések magas száma miatt több vezető technológiai vállalat is, például a *Google* és a *Facebook* is betiltotta az ICO-hirdetéseket.[36]

Az ICO-k szabályozása a *kriptovalutákhoz* hasonló módon országonként eltérő. Eddig a leghatározottabb fellépés Kína részéről történt, mert a központi bank illegálisnak minősítette az ICO-n keresztüli tőkebevonást, és ezek azonnali beszüntetését rendelte el.[37] Érdemes megemlíteni Máltát, ahol egy hiánypótló törvénycsomagot fogadtak el, amely részletesen szabályozza a virtuális eszközöket, szem előtt tartva a befektetők védelmét.[38]

Mindezekre tekintettel megállapítható, hogy a *kriptovalutával* összefüggésben elkövetett vagyon elleni bűncselekmény minősítése a Btk. 373. §-ában szabályozott, hagyományos értelemben vett csalásnak felelhet meg. Ezzel kapcsolatban fontos a kár – mint tényállási elem – fogalmával részletesen foglalkozni. A büntetőjog a kár fogalmának tartalmi elemeit a polgári jogtól eltérően határozza meg.[39] A va-

[33] Györfi András: Az ICO – Így indul útjára egy kriptopénz. In: Györfi András (szerk.): *Kriptopénz ABC.* HVG Könyvek, Budapest, 2019, 102.

[34] Györfi: i. m., 108.

[35] Az Egyesült Államokban az *FBI* letartóztatta az *AriseBank* igazgatóját azért, mert a befektetőket tévedésbe ejtve 4 millió dollár értékben kárt okozott nekik. A vád szerint a vállalkozását „az első decentralizált banki platformként" hirdette, különböző szolgáltatásokkal, de ezekre vonatkozóan nem rendelkezett engedélyekkel. Saját *AriseCoin* virtuális fizetőeszközének kibocsátásával gyűjtött pénzt, majd ezt az összeget magáncélra költötte el. Department of Justice, U.S. Attorney's Office, Northern District of Texas, 2018. https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million (2019. 01. 15.).

[36] Györfi: i. m., 104.

[37] Egri Szilvia: *A kriptovaluták világának legfrissebb fejleményei: figyelmeztetés, tiltás, bezárás.* Fintechzone, 2017. 10. 06. https://fintechzone.hu/kriptovalutak-legfrissebb-fejlemenyek/ (2019. 01. 31.).

[38] A csomag egy-egy törvényt tartalmaz az innovatív technológiai megoldásokról és szolgáltatásokról, a Máltai Digitális Innovációs Hatóságról és a virtuális pénzügyi eszközökről. Bujtár Zsolt: A kriptovaluták európai és máltai szabályozásának az összehasonlítása – A máltai sólyom szárnyalása. *Európai Jog,* 2018/5, 12–13.

[39] Deák Zoltán: A kár büntetőjogi fogalmáról – megjegyzések egy eseti döntés margójára. *Magyar Jog,* 2012/6, 369–374.

gyon fogalmát pedig sem a Btk., sem a Ptk. nem határozza meg, azonban a Btk. a vagyonelkobzáshoz kapcsolódóan a vagyon fogalma alá vonja a vagyon hasznát, a vagyoni értékű jogot, a követelést, továbbá bármely pénzben kifejezhető értékkel bíró előnyt is.[40] Az 1/2008. BJE határozat indokolása szerint a vagyon – a bűncselekményből eredő, illetve azzal összefüggő – pénzben kifejezhető értékkel bíró javakat és azok hasznát is magában foglalja. Ezt figyelembe véve úgy gondolom, hogy a *kriptovalutára* is mint vagyonelemre tekinthetünk, és ezért vagyonelkobzás tárgyát képezheti. A vagyon fogalmának meghatározásával pedig azért kell foglalkozni, mert az a kár fogalmánál is megjelenik. A kár a Btk. 459. § (1) bekezdésének 16. pontja szerint a bűncselekménnyel a vagyonban okozott értékcsökkenést jelenti. Ez a csalás bűncselekménye esetén kiegészül azzal, hogy kárnak kell tekinteni az igénybe vett szolgáltatás meg nem fizetett ellenértékét is.[41] A kár, pénzben kifejezhető, összegszerűen meghatározható anyagi értéknagyság.[42] Ezzel összefüggésben meg kell állapítani, hogy a virtuális fizetőeszközök a piaci viszonyok között konkrétan – egy adott időpontra vonatkozóan – kiszámítható, valódi pénzben kifejezhető értékkel rendelkeznek, így a kár – és a vagyoni hátrány – megállapításánál értékelhetők.[43]

1.2. A pénzmosás és a terrorizmus finanszírozása

A pénzmosás kihívás elé állítja a jogalkotókat, különösen a virtuális fizetőeszközök korában, ami a korábbiaknál sokkal kifinomultabb, nehezebben követhető módot nyújt az illegálisan szerzett jövedelmek tisztára mosására.

A *kriptovaluták* használata pénzmosási és terrorizmusfinanszírozási kockázatokat hordoz magában, ami a decentralizált infrastruktúra és a *pszeudoanonim* tranzakciók eredménye. A tranzakciók szolgálhatják legális üzleti műveletek elszámolását, de illegális tevékenységekét is.

A bűncselekményből származó pénzek tisztára mosására alkalmas azok *kriptovalutára* történő átváltása, majd különböző címekre való továbbutalása.

A pénzmosás valamennyi fázisa a virtuális fizetőeszközök használata során is – a fiat pénzekhez hasonló módon – megvalósulhat.

Az elhelyezést a *kriptovaluták* megkönnyítik, mert anonim módon jelentős számú pénztárcát lehet létrehozni költségmentesen, vagy alacsony költség és kockázat mellett.

A rétegzés (bújtatás) megvalósul a többszöri átutalásokkal különböző pénztárcák között és/vagy különböző kriptovaluták és fiat pénzek, vagy kriptovaluták és kriptovaluták közötti átváltással. Az *atomic swap* technológiai fejlesztés pedig még inkább elősegítheti a *kriptovalutákkal* kapcsolatos visszaéléseket.

Az integráció megtörténhet közvetlenül, a virtuális fizetőeszközök árukra és szolgáltatásokra való váltásával, vagy pedig közvetve fiat pénz útján, amit elősegít mind-

[40] Btk. 76. §.
[41] Btk. 373. § (7).
[42] Molnár (2009): i. m., 702.
[43] Eszteri (2017): i. m., 30.

azon áruk és szolgáltatások egyre növekvő száma, amelyekért a *kriptovalutákat* fizetőeszközként elfogadják. A másik megoldás a kriptovalutákba történő befektetés. Az intézményi befektetők számára is egyre inkább vonzóbbá vált a virtuális fizetőeszközök piaca, amelyre befektetési, valamint kereskedési (spekulációs) szándékkal lépnek be. Ez a lépés jelentős likviditást biztosít ezeknek a piacoknak.

Hasonlóképp, az olyan ICO-k is alkalmasak a bűnös eredetű pénz legalizálására, amelyeknél gyenge az ügyfélellenőrzés, és ezt a bűnelkövetők kihasználhatják, a virtuális fizetőeszköz portfóliójukat más *tokenekké* alakítják az ICO-n keresztüli jegyzésekkel. A végső cél ez utóbbi esetén az, hogy a kriptotőzsdére bevezetésre került *tokenekből* vagy a más virtuális fizetőeszközökben lévő befektetéseket kivegyék.[44]

A *kriptovaluták* átváltásával kapcsolatban különböző szolgáltatások érhetők el, amelyek a tranzakciók nyomon követhetőségét megnehezíthetik. Így, a már említett virtuális pénzváltó platformok (például Kraken, Coinbase, Bitstamp) a kriptovaluták és a törvényes fizetőeszközök közötti átváltást segítik. Ezek nyílt és átlátható módon, online működő szolgáltatók (például ügyfélazonosítással, részletes felhasználási feltételekkel rendelkeznek). Ezenkívül vannak a *Darknet* fórumokon elérhető, ún. *mixing* vagy *tumbling* szolgáltatások, amelyek vagy egy közös, nagyobb összeget tartalmazó címet bontanak fel kisebbekre, vagy fordítva, több kisebb összeget egyesítenek egy közös címen.[45] A céljuk ezzel az, hogy a többlépcsős tranzakciók lebonyolítása révén az eredeti forrás és az új *kriptovaluta* cím közötti kapcsolatot elrejtsék annak érdekében, hogy azt ne tudják azonosítani. Gyakran ezek a szolgáltatók azzal reklámozzák magukat, hogy a tranzakciók előzményeit is törlik rövid időn belül. A *ShapesShift* a különböző *kriptovaluták* közötti átváltást biztosítja, ennek használata már regisztrációhoz kötött.[46] Az *atomic swap* használatával harmadik fél közbeiktatása nélküli, más *kriptovalutára* történő átváltásra van lehetőség, okosszerződés révén.

2013 óta az Egyesült Államokban a *kriptovalutákkal* kapcsolatos szolgáltatást nyújtó vállalkozások gyakorlatilag azonos megítélés alá esnek a pénzügyi szolgáltatást nyújtó egyéb vállalkozásokkal.[47]

Az Európai Unióban azonban a kriptováltó szolgáltatóknak ez idáig nem volt uniós kötelezettségük arra, hogy a gyanús tevékenységeket azonosítsák, így a bűnelkövetők – és akár a terrorista csoportok is[48] – pénzt utalhattak az uniós pénzügyi rendszerbe vagy a virtuális fizetőeszköz rendszereken belül azáltal, hogy elrejtették az átutalásokat, valamint magas fokú anonimitást élveztek ezeken a platformokon.

[44] Poskriakov, Fedor–Chiriaeva, Maria–Cavin, Christophe: Cryptocurrency compliance and risks: a European KYC/AMLP perspective. In: Dewey, Josias (ed.): *Blockchain & Cryptocurrency Regulation 2019*. Global Legal Group, 2019, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/13-cryptocurrency-compliance-and-risks-a-european-kycaml-perspective (2019. 02. 03.).

[45] Eszteri (2017): i. m., 27.

[46] https://shapeshift.io/.

[47] *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Guidance.* Department of the Treasury, Financial Crimes Enforcement Network, 2013. https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (2019. 08. 30.).

[48] Az *Europol* jelentése szerint megfigyelhető a terrorizmusfinanszírozás terén a *kriptovaluták* használata, azonban az ismert esetek száma alapján ez még nem számottevő. *European Union Terrorism Situation and Trend Report 2018*. Europol, 2018, 12.

Erre reflektál az EU ötödik pénzmosás elleni irányelve,[49] amelynek nóvuma, hogy először határozza meg a virtuális fizetőeszköz fogalmát. A 3. cikk 19. pont értelmében: *„olyan digitális értékmegjelenítés, amelyet nem központi bank vagy közigazgatási szerv bocsát ki vagy garantál, nem feltétlenül kapcsolódik rendeleti pénzekhez, és nem rendelkezik rendeleti pénz vagy pénz jogi státuszával, de természetes vagy jogi személyek elfogadják csereértékként, valamint elektronikusan átutalható, tárolható és lehet vele elektronikusan kereskedni".* Továbbá a virtuális fizetőeszközök nem tévesztendők össze az elektronikus pénzzel,[50] a pénz átfogóbb fogalmával,[51] az (EU) 2015/2366 irányelv 3. cikkének *k)* és *l)* pontjában meghatározottak szerint mentesített eszközökön tárolt monetáris értékkel, illetve a kizárólag egy adott játékkörnyezeten belül használható, játékalapú fizetőeszközökkel. Bár a virtuális fizetőeszközöket gyakran használják fizetőeszközként, azok más célokra is felhasználhatók és szélesebb körben alkalmazhatók, például csereeszközként, befektetési eszközként, értéktároló termékként vagy online kaszinókban. Az ötödik pénzmosás elleni irányelv célja a virtuális fizetőeszközök valamennyi lehetséges felhasználásának szabályozása.

Jelentős lépésnek számít, hogy a hatályát kiterjesztették további kötelezett szolgáltatókra is, akik a virtuális fizetőeszközök és a rendeleti pénzek közötti átváltással foglalkoznak, valamint a letétkezelő pénztárca-szolgáltatókra. Utóbbi fogalmát a 3. cikk 19. pontja határozza meg: *„olyan szervezet, amely ügyfelei nevében virtuális fizetőeszközök tartására, tárolására és átutalására szolgáló kriptográfiai magánkulcsok megőrzésével kapcsolatos szolgáltatást nyújt".*

Az új szabályozás lényegét tekintve abból indul ki, hogy a virtuális fizetőeszközök rendszere decentralizált, mert nincs központi felügyeleti szervük, ezért nem lehet kihez fordulni a tranzakciókkal kapcsolatos információkért. Azonban az ötödik pénzmosás elleni irányelvben szabályozott szolgáltatók segítségével a kriptográfiai kulcsok – vagyis a címek és privát kulcsok – a regisztrált ügyfelekhez tartoznak, akik ezáltal beazonosíthatók, és ezen szolgáltatók biztosíthatják a tranzakciókra vonatkozó további adatokat a hatóságok részére, azokban az esetekben, amikor a felhasználók igénybe vesznek ilyen jellegű szolgáltatásokat.

A cél, hogy a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem érdekében az illetékes hatóságok képesek legyenek arra, hogy a kötelezett szolgáltatók révén nyomon kövessék a virtuális fizetőeszközök használatát. Az irányelv a kötelezett szolgáltatókkal szemben az ún. „ismerd meg az ügyfeledet" (*Know Your Customer,*

[49] Az Európai Parlament és a Tanács (EU) 2018/843 irányelve (2018. május 30.) a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról. HL L 156, 19.6.2018, 43–74.

[50] Az Európai Parlament és a Tanács 2009/110/EK irányelv 2. cikkének 2. pontjában meghatározott *elektronikus pénz: „a kibocsátóval szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – monetáris érték, amelyet pénzeszköz átvételével bocsátanak ki a 2007/64/EK irányelv 4. cikkének 5. pontjában meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikus-pénz-kibocsátón kívül más természetes vagy jogi személy is elfogad".*

[51] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelv 4. cikkének 25. pontjában meghatározott *pénz: „bankjegyek és pénzérmék, számlapénz, vagy a 2009/110/EK irányelv 2. cikke 2. pontjában szereplő meghatározás szerinti elektronikus pénz".*

avagy *KYC*) követelményt támasztja, ami a meghatározott ügyfél-átvilágítási eljárás segítségével elősegíti a pénzmosási és a terrorizmusfinanszírozási kockázat csökkentését, az ügyfelek azonosítása és kilétének ellenőrzése révén. A kötelezett szolgáltatóknak a lehető legtöbb adatot be kell gyűjteniük az ügyfeleikről annak érdekében, hogy tisztában legyenek azok tevékenységével, üzleti kapcsolataik jellegével, pénzügyi szokásaikkal. Az ügyfélmegismerés és a tranzakció monitoring együttesen biztosíthatja a rendszer átláthatóságát. Az átváltó és pénztárca-kezelő szolgáltatók esetében a következő intézkedések fontosak: az ügyfél azonosítása a felhasználói fiók nyitásakor, nyilvántartás vezetése és beszámolók készítése, gyanús tevékenységek jelentése, belső szabályozási rendszer kiépítése (például belső szabályzatok, képzések, *compliance officer* alkalmazása stb.).[52]

Az ötödik pénzmosás elleni irányelv 47. cikkének (1) bekezdése értelmében a tagállamok kötelezettsége, hogy biztosítsák a virtuális fizetőeszközök és rendeleti pénzek közötti átváltási szolgáltatásokat nyújtó szolgáltatók, valamint a letétkezelő pénztárca-szolgáltatók nyilvántartásba vételét. Azonban érdemes kitérni arra, hogy a virtuális fizetőeszközök egymás közötti átváltását biztosító szolgáltatókra, valamint a kriptotőzsdékre és a kereskedési platformokra nem terjed ki a hatálya.

Megállapítandó, hogy ez nem oldja meg teljes mértékben a virtuális fizetőeszközökkel végrehajtott műveletek anonimitásával kapcsolatos problémákat, mivel a felhasználók az ilyen szolgáltatók igénybevétele nélkül is végezhetnek műveleteket, hiszen nem kell azokat szükségszerűen átváltani törvényes fizetőeszközre. Az anonimitással kapcsolatos kockázatok elleni küzdelem érdekében lehetővé kell tenni a nemzeti pénzügyi információs egységek számára az ahhoz szükséges információk begyűjtését, hogy a virtuális fizetőeszköz címét a virtuális fizetőeszköz tulajdonosának kilétével tudják társítani. Emellett tovább kell vizsgálni annak lehetőségét, hogy a felhasználók önkéntes önbevallás formájában nyilatkozatot tehessenek a kijelölt hatóságoknak.

Az ötödik pénzmosás elleni irányelvet a tagállamok kötelesek 2020. január 10-ig átültetni a nemzeti jogukba. A Bizottság 2022. január 11-ig, majd azt követően háromévente jelentést készít a végrehajtásáról, és benyújtja azt az Európai Parlamentnek és a Tanácsnak. Az első jelentéshez, amelyet 2022. január 11-ig tesznek közzé, szükség esetén megfelelő jogalkotási javaslatokat kell mellékelni, ideértve adott esetben a virtuális fizetőeszközökkel, a felhasználók kilétét és a pénztárcacímeket rögzítő, a pénzügyi információs egységek számára hozzáférhető központi adatbázis létrehozására és fenntartására vonatkozó felhatalmazásokkal, valamint a virtuális fizetőeszközök felhasználói számára kidolgozott nyilatkozatmintákkal és a tagállami vagyonvisszaszerzési hivatalok közötti együttműködés javításával, illetve a 20. cikk *b)* pontjában említett intézkedések kockázatalapú alkalmazásával kapcsolatban.

[52] Érdekesség, hogy az Egyesült Államok adóhatósága, az *Internal Revenue Service (IRS)* és az Igazságügyi Minisztérium Adóosztálya egymással együttműködve kiadta és érvényesítette az első virtuális fizetőeszközzel kapcsolatos *„John Doe"* idézést a világ egyik legnagyobb kriptotőzsdéjével *(Coinbase)* szemben. Ennek eredményeképpen a szolgáltató köteles volt átadni a 20 000 $ kereskedési forgalom feletti fiókokra vonatkozó ügyféladatokat. Ez azért fontos, mert elősegítheti az ügyfelek azonosítását és a nyomozás eredményes lefolytatását. *United States v. Coinbase, Inc. et al., Order Regarding Petition to Enforce IRS Summons at 14 (Doc. 78), Case No. 3:17-cv-01431 (N.D. Cal.).*

Érdekességként megemlítendő, hogy korábban csak egyetlen alkalommal került sor uniós szintű döntésre a virtuális fizetőeszközökkel kapcsolatban. Ennek során az Európai Unió Bírósága foglalkozott a *bitcoin* jogi értékelésével, méghozzá egy adózás kapcsán előterjesztett előzetes döntéshozatali eljárásban. 2015-ben a Bíróság állást foglalt arról, hogy a *bitcoinok* nemzeti (hivatalos) devizára való váltása áfaköteles vagy áfamentes tevékenységnek minősül-e. A Bíróság megállapította, hogy a hagyományos devizák *bitcoinra* való át- és visszaváltása ellenérték fejében teljesített szolgáltatásnyújtásnak minősül. Tekintettel arra, hogy a *bitcoin* virtuális devizának nincs más célja, mint az, hogy fizetőeszközként használják, és e tekintetben egyes gazdasági szereplők elfogadják azt, ezért a Bíróság úgy döntött, hogy indokolt az adómentesség alkalmazása a *bitcoin* és a hagyományos devizák átváltására irányuló szolgáltatás esetén is. Az ítélet a *bitcoinra* következetesen a „virtuális deviza" kifejezést használja. Az a Bíróság szerint a 2009/110/EK irányelvben meghatározott elektronikus pénztől annyiban különbözik, hogy az összegeket nem hagyományos számítási egységben, hanem olyan virtuális egységben fejezi ki, mint a *bitcoin.*[53]

A következőkben a pénzmosás hazai szabályozását vizsgálom, a *kriptovalutákra* tekintettel. Először a pénzmosás elkövetési tárgyával foglalkozom, amely a bűncselekményként büntetendő cselekményből származó dolog. A dolog fogalmát sem a Btk., sem a Ptk. külön nem definiálja, hanem a pénzmosásról, a bűncselekményből származó dolgok felkutatásáról, lefoglalásáról és elkobzásáról szóló, Strasbourgban, 1990. november 8-án kelt egyezmény értelmező rendelkezése határozza meg az 1. cikk *b)* pontjában, amely szerint a dolog *„bármilyen dolog lehet, legyen az megfogható vagy megfoghatatlan, ingó vagy ingatlan, illetve olyan jogi irat vagy okmány, amely az ilyen dolgokra vonatkozó jogosultságot, vagy ahhoz fűződő érdeket igazol".* Ez a fogalommeghatározás a pénzmosás tényállásának alkalmazása során közvetlenül érvényesítendő.

A Ptk. az 5:14. § (1) bekezdésében annyit rögzít, hogy a birtokba vehető testi tárgy tulajdonjog tárgya lehet. A Btk. a 402. § (1) bekezdésében foglalt értelmező rendelkezés értelmében a pénzmosás tényállása *„alkalmazásában dolgon a vagyoni jogosultságot megtestesítő olyan okiratot, dematerializált értékpapírt is érteni kell, amely a benne tanúsított vagyoni érték vagy jogosultság feletti rendelkezést önmagában, illetve dematerializált formában kibocsátott értékpapír esetén az értékpapírszámla jogosultjának biztosítja".*

Szathmáry Zoltán a *kriptovalutáknak* számítástechnikai adatként való kezelését tartja elfogadhatónak – a megfelelő polgári jogi besorolás hiányában – a büntető anyagi és eljárásjogi szabályok szempontjából.[54] A *kriptovaluta* egy vagyoni értéket megtestesítő számítástechnikai adat, amelyet fizetésre használnak. *Szathmáryval* egyetértve, megítélésem szerint is a megoldást a dolog fogalmának értelmező rendelkezés keretében történő kiterjesztése jelentené. Javaslata szerint ez a következőképpen történne: *„vagyoni értéket önmagában vagy feldolgozása révén biztosító, fizetésre használt elektronikus adat vagy adatok összessége, ideértve a fizetés elektronikus nyilvántartási egységét is".*[55]

[53] *C-264/14. sz. Skatteverket kontra David Hedquist ügy,* 2015. október 22-ei ítélet.

[54] Szathmáry (2015): i. m., 644.

[55] Szathmáry (2015): i. m., 646.

A másik kérdés az elkövetési magatartással függ össze, méghozzá a saját pénzmosás esetén a dolog eredetének eltitkolása, elleplezése céljából pénzügyi tevékenység végzése, vagy pénzügyi szolgáltatás igénybevétele. Ezt a Btk. 402. § (2) bekezdésében foglalt értelmező rendelkezéssel határozza meg. Ez azért is fontos, mert az elkövetők gyakran különböző átváltó vagy pénztárca-kezelő szolgáltatókat vesznek igénybe, amelyeken keresztül utalásokat végeznek vagy átváltják a *kriptovalutákat.* Felmerül a kérdés, hogy ezen szolgáltatók tevékenysége pénzügyi szolgáltatási vagy kiegészítő pénzügyi szolgáltatási tevékenységnek minősül-e, a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény értelmében. Jelenleg azonban még nem minősül annak. Ez rámutat arra, hogy nemcsak a *kriptovalutát* kell a jognak kezelnie, hanem a használatához köthető tevékenységeket és a hasznosítási formáit is, például a fizetési rendszer működtetést, kereskedési felület üzemeltetést, bányászatot, tárolást, vagy a *kriptovaluta*-alapú származtatott termékeket. Ezek a tevékenységek jelenleg nem illeszthetők be maradéktalanul a pénzügyi jogi tárgyú törvényeink fogalmi rendszerébe, ezért azok módosítására, kiegészítésére lesz szükség.

Virtuális fizetőeszközök bevonásával olyan hagyományos és jól ismert pénzmosási módszerek is új színezetet kaphatnak, mint az ún. *money mule* jelenség. Ebben az esetben az elkövetők magukat virtuális pénzváltó platformok képviselőjének kiadva munkaszerződést ajánlanak, amelynek keretében a megkeresett fél „munkája" annyi lenne, hogy saját fizetési számláján a pénzváltótól származó jelentősebb összegeket kell fogadnia, majd azt készpénzben felvenni, vagy a „munkáltató" által megadott fizetési számlákra tovább utalni, természetesen jutalékért cserébe. Aki ilyen jellegű ajánlatot elfogad, maga is érintetté válik a pénzmosás gondatlan alakzatának elkövetésében.[56]

1.3. Zsarolás

A zsarolás eredmény-bűncselekmény, amelynek az eredménye a vagyoni hátrány, amely a Btk. 459. §-a (1) bekezdésének 17. pontja értelmében a vagyonban okozott kárból és az elmaradt vagyoni előnyből tevődik össze. A zsarolás hagyományos bűncselekménytípus, de a technológiai fejlődésnek köszönhetően már az infokommunikációs technológia és a virtuális fizetési rendszerek felhasználásával is elkövethető. Általában az informatikai környezetben e bűncselekmény az elkövetők részéről fenyegetéssel valósul meg, például *DDoS*-támadások indítását vagy zsarolóvírus által a titkosított adatok törlését vagy a jogosulatlanul megszerzett személyes adatok nyilvánosságra hozatalát helyezik kilátásba, majd a „váltságdíjat" *kriptovalutákban* kérik.[57]

[56] Éves jelentés – 2016. év. Nemzeti Adó- és Vámhivatal Központi Irányítása Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda, Budapest, 2016, 15.

[57] Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In: Sárközy Tamás (szerk.): *A Magyar Jogász Egylet 2018. évi tudományos pályázatán díjat nyert pályázatok.* Magyar Jogászegyleti Értekezések 2018/9–10. Magyar Közlöny Lap- és Könyvkiadó, Magyar Jogász Egylet, Budapest, 2018, 169.

1.4. Az információs rendszer elleni bűncselekmények

A *kriptovaluták* népszerűsége a bűnelkövetők számára új célpontokat is szolgáltat: a *kriptovaluta*-felhasználókat, a már említett átváltó és letétkezelő, pénztárcakezelő szolgáltatókat, valamint kriptotőzsdéket és befektetési szolgáltatókat, akiket – a pénzintézetekhez és azok ügyfeleihez hasonló módon – adathalász kísérletekkel, rosszindulatú programok használatával vagy *hacking* útján támadnak az értékes adatokért, így különösen a privát kulcsok és a pénztárcafájlok megszerzése érdekében.[58] A fizetésre használható, virtuális pénztárcák bármilyen eszközön vagy az online pénztárca-szolgáltatóknál tárolhatók, így – hasonlóan más digitálisan tárolt adatokhoz – a hozzá tartozó kódok esetleges feltörésével vagy azok megszerzésével a virtuális fizetőeszköz hozzáférhetővé, így ellophatóvá válik.

Ezekben az esetekben a digitális környezet elengedhetetlenül szükséges a *kriptovalutákkal* kapcsolatos visszaélések elkövetéséhez, így indokolt ezeket a virtuális „lopásokat" informatikai bűncselekményként értékelni.[59] Érdemes azonban megjegyezni, hogy a lopás tényállása megvalósulhat, amennyiben a *kriptovalutát* hardveres pénztárcán, azaz *offline* tárolják, és azt veszik el.[60]

Az elkövető a Btk. 375. §-ába ütköző információs rendszer felhasználásával elkövetett csalást valósítja meg, amennyiben megszerzi a virtuális pénztárcát, azaz a *wallet.dat* fájlt, vagy az *online* pénztárca-szolgáltatónál tárolthoz hozzáfér egy kibertámadás következtében. Ebben az esetben az adott tárcához tartozó *kriptovalutával* is rendelkezni tud, így amennyiben pénzügyi műveletet hajt végre, akkor ezzel kárt okoz. A letétkezelő pénztárca-szolgáltatókkal és átváltókkal szemben elkövetett támadások gyakoriak (például az *Mt. Gox* és a *Coincheck* esete).[61] Az információs rendszer elleni bűncselekmények elkövetési tárgyaként mint számítástechnikai adat jelenik meg a virtuális pénztárca. A károkozás hiányában a 423. § szerinti információs rendszer vagy adat megsértésének deliktumáért vonható felelősségre a terhelt, akkor, ha a szolgáltatóktól jogosulatlanul megszerzi a felhasználói adatokat, majd azokat felhasználja. A másik egyre gyakoribb eset az ún. *cryptojacking,* ami olyan folyamatot takar, amelynek során a jogosult felhasználó engedélye nélkül a számítógépnek a feldolgozási sebességét vagy sávszélességét használják célzottan *kriptovaluta* bányászatra (például ez történhet *malware* fertőzés révén vagy a felhasználó által meglátogatott honlapba beépítve).[62]

---

[58] Lásd az *Europol* idézett jelentését (2018), 8.; valamint Simon Béla: Kriptovaluták – rendészeti válaszok. *Belügyi Szemle,* 2018/10, 83.

[59] Eszteri Dániel: *A World of Warcraft-tól a Bitcoin-ig*: *Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben*. PhD-értekezés, Pécs, 2015, 205. A lopás tényállása megvalósulhat, amennyiben a kriptovalutát hardveres pénztárcán, azaz offline tárolják, és azt veszik el. Miskolczi Barna–Szathmáry Zoltán: *Büntetőjogi kérdések az információk korában.* HVG-ORAC, Budapest, 2019, 163.

[60] Miskolczi–Szathmáry: i. m., 163.

[61] Az *Mt. Gox* és a *Coincheck* japán kriptotőzsdék 2014-es, illetve 2018-as támadása során az elkövetők több száz millió dollár értékben jutottak hozzá *kriptovalutákhoz,* és ennek hatására szigorodott a japán szabályozás. Például fontos követelménnyé vált, hogy a regisztrált tőzsdék esetén az ügyfelek eszközei elkülönüljenek a tőzsdéétől. Az *Mt. Gox* esetén a kettő még azonos volt. A jelenlegi szabályozásnak köszönhetően naponta kell ellenőrizniük, hogy rendelkeznek-e megfelelő fedezettel.

[62] Lásd az *Europol* idézett jelentését (2018), 19.

A rosszindulatú program készítője, valamint az a terhelt, aki a privát kulcsot átadja, hozzáférhetővé teszi, megszerzi, vagy forgalomba hozza, az a 424. § szerinti információs rendszer védelmét biztosító technikai intézkedés kijátszásáért felel.

Továbbá e körben kell foglalkozni a legújabb uniós szabályozással, ugyanis elfogadásra került a 2019/713 számú irányelv (a továbbiakban: 2019-es irányelv)[63] a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelem elősegítése érdekében, amely felváltotta a korábbi tanácsi kerethatározatot. Ennek bevezetése azzal magyarázható, hogy a meglévő szabályozást frissíteni és kiegészíteni kellett – különös tekintettel a számítógépes csalásra – e bűncselekményekkel kapcsolatos, a büntetésekre, a megelőzésre, a sértettek segítésére, valamint a határon átnyúló együttműködésre vonatkozó további rendelkezésekkel. Ezt indokolta továbbá az is, hogy e területen az egyes tagállamok büntetőjogi szabályozása hiányos, valamint a tényállások között jelentős eltérések voltak tetten érhetők, és ezért szükségessé vált ezek egymáshoz közelítése.

A 2019-es irányelv minimumszabályokat ír elő, ezért a tagállamok ennél szigorúbb büntetőjogi szabályokat is elfogadhatnak. Továbbá közös fogalommeghatározásokat is nyújt, amelyeknek ki kell terjedniük a készpénz-helyettesítő fizetési eszközök olyan új típusaira is, amelyek lehetővé teszik az elektronikus pénz és a virtuális fizetési eszközök átutalását. A 2. cikk *a)* pontja értelmében *„a készpénz-helyettesítő fizetési eszköz olyan immateriális vagy materiális védett készülék, tárgy vagy rögzített adat, vagy ezek kombinációja, ide nem értve a törvényes fizetőeszközöket, amely önállóan, illetve egy eljárás vagy eljárások alkalmazásával lehetővé teszi, hogy birtokosa vagy felhasználója pénzt vagy pénzbeli értéket utaljon át, többek között digitális csereeszközök révén”.* Erre tekintettel büntetőjogi védelmet kizárólag az olyan fizetési eszközök kapnak, amelyek speciális védelmi jellemzőkkel vannak ellátva, tehát a 2. cikk *b)* pont szerint az utánzással vagy csalárd felhasználással szemben, például tervezés, kódolás vagy aláírás útján védett készüléknek, tárgynak vagy rögzített adatnak minősülnek. Ezáltal a gazdasági szereplőket is arra kívánják ösztönözni, hogy az általuk kibocsátott fizetési eszközöket megfelelő védelemmel lássák el.

A készpénz-helyettesítő fizetési eszközök fogalmába bele kell foglalni, hogy a készpénz-helyettesítő fizetési eszköz több különböző, együttesen ható elemből állhat, például egy fizetési mobilalkalmazásból és egy ahhoz társuló engedélyezésből (jelszó). A készpénz-helyettesítő fizetési eszközök fogalmát a 2019-es irányelv azzal az értelmezéssel alkalmazza, hogy az eszköz ténylegesen lehetővé teszi, hogy birtokosa vagy felhasználója pénzt vagy pénzbeli értéket utaljon át, vagy fizetési megbízást kezdeményezzen, tehát annyiban alkalmazandó, amennyiben az eszköz fizetési funkciójáról van szó. Így például egy fizetési mobilalkalmazásnak a hozzá tartozó szükséges engedélyezés nélküli, jogellenes megszerzése nem minősül készpénz-helyettesítő fizetési eszköz jogellenes megszerzésének, mivel ténylegesen nem teszi lehetővé felhasználója számára pénz vagy pénzbeli érték átutalását.

[63] Az Európai Parlament és a Tanács (EU) 2019/713 irányelve (2019. április 17.) a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról. HL L123/18, 2019.5.10.

Mindezen kívül az egyik legnagyobb újdonság, hogy a 2019-es irányelv hatálya kiterjed a virtuális fizetési eszközök – azaz a *kriptovaluták* – átutalását lehetővé tevő digitális pénztárcákra is. A 2. cikk *d)* pontja szerint digitális csereeszköz az elektronikus pénz és a virtuális fizetési eszköz, utóbbi fogalommeghatározását a korábban elfogadott ötödik pénzmosás elleni irányelv vette át. A „digitális csereeszközök" fogalommeghatározásával ennek az irányelvnek el kell ismernie, hogy a virtuális fizetési eszközök átutalására szolgáló digitális pénztárcák rendelkezhetnek – de nem szükségszerűen rendelkeznek – a fizetési eszközök sajátosságaival, és nem terjeszthetik ki a fizetési eszköz fogalommeghatározását.

1.5. Piramisjáték szervezése

Az egyes bűnelkövetői körök látszólag virtuális fizetőeszközökbe történő befektetést és irreálisan magas hozamokat ígérnek, a virtuális fizetőeszközöket egyfajta hívószóként alkalmazzák. Tevékenységük hagyományos piramisjáték, azonban a piramisjátékokhoz hasonlóan kézzelfogható, tényleges belső értéket hordozó termék vagy eszköz nem található, a hátterében pedig jellemzően egy *offshore* cég áll.

Ehhez érdemes megemlíteni az ún. *OneCoin-t,* mely konstrukció látszólag valamiféle eszközbe történő befektetést tesz lehetővé, valójában azonban kereskedni kizárólag a tevékenységet szervező által üzemeltetett, zárt és nem ellenőrizhető fórumon van mód, valamint az állítólagos virtuális fizetőeszköz értéke, árfolyama objektíven megállapíthatatlan. A rendszerbe magas hozamokat ígérve szerveznek az interneten keresztül új belépőket, olyan módon, hogy utóbbiak befizetéseiből a korábban csatlakozottaknak – akiknek így erőteljes anyagi érdeke a marketing és a toborzás – jutalékot fizetnek.[64]

Ez a Btk. 412. §-ában szabályozott piramisjáték szervezésének felel meg, amely szerint, *„aki mások pénzének előre meghatározott formában történő, és kockázati tényezőt is tartalmazó módon való összegyűjtésén és szétosztásán alapuló olyan játékot szervez, amelyben a láncszerűen bekapcsolódó résztvevők a láncban előttük álló résztvevők számára közvetlenül, vagy a szervező útján pénzfizetést vagy más szolgáltatást teljesítenek, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő".*

2. A *kriptovalutákkal* összefüggő büntetőeljárás-jogi kérdések

A *kriptovaluták* egységes szabályozásának és jogi besorolásuknak a hiánya büntetőeljárás-jogi szempontból is kihívást jelent, mivel felmerül a kérdés, hogy lefoglalás tárgyát képezhetik-e, vagy sem. Az Egyesült Államokban és az Egyesült Királyság-

[64] *OneCoin* értékesítésre Magyarországon is sor került, ezért az MNB Piacfelügyeleti munkacsoportja is folyamatosan megfigyelés alatt tartja ezt a sémát. Az MNB egyúttal közös fellépésről egyeztetett a Belügyminisztérium és a rendőrség különböző szerveivel, az adóhatósággal, illetve ügyészségi vezetőkkel. https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/a-onecoin-elleni-fellepesrol-targyalt-a-piacfelugyeleti-munkacsoport (2019. 01. 15.).

ban is sor került *kriptovaluták* lefoglalására,[65] valamint Dél-Koreában a legfelsőbb bíróság először hozott a *kriptovalutákkal* kapcsolatban döntést, amelyben mérhető értékkel rendelkező eszközöknek tekinti azokat, és mivel értékkel rendelkeznek, ezért lefoglalhatók.[66]

A büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) szabályozása szerint lefoglalni az ingó dolgot, a számlapénzt, az elektronikus pénzt vagy az elektronikus adatot lehet.[67] A jövőben a decentralizált virtuális fizetőeszközök elektronikus adatként lefoglalás tárgyát képezhetik. A Be. 315. § (1) bekezdése értelmében az elektronikus adat lefoglalása történhet az elektronikus adatról való másolat készítésével, áthelyezésével, az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével, vagy ezek lefoglalásával. A 315. § (2) bekezdésének értelmében a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, ha olyan műveletet végeznek, amely végül is a vagyoni érték feletti rendelkezési lehetőségét akadályozza meg, ezzel kialakítva az ún. virtuális vagyontárgyak biztosításának keretszabályát.[68]

A *kriptovaluták* esetében problémát jelent az, hogy a jogosult soha nincs fizikai birtokában a *kriptovaluta*-egységeinek. Mindenképpen a privát kulcsra van szükség ahhoz, hogy azokkal rendelkezni lehessen. Éppen ezért az áthelyezés, másolatkészítés és az információs rendszerek vagy adathordozók lefoglalása sem vezethet feltétlenül eredményre, mert ugyan a pénztárcafájlt átmásolhatják vagy a lefoglalt eszközt (például hardver pénztárca) elvonhatják, azonban fennállhat annak a veszélye, hogy a jogosult előzőleg biztonsági másolatot készített róla, és akkor továbbra is rendelkezhet a *kriptovaluta* egyenlege felett. A másik probléma, hogy a privát kulcs nélkül a hatóság nem tud hozzáférni a *kriptovaluta*-egységekhez, a gyanúsított pedig nem köteles ezeket átadni a nyomozó hatóság számára. Éppen ezért különösen nagy körültekintést igényel a nyomok felkutatása (például az információs rendszeren belül kutatva a pénztárcafájl, valamint a többi pénztárcatípus vagy privát kulcs után).[69] Mindez következik abból, hogy a büntetőeljárásban az önvádra kötelezés tilalma érvényesül, ami azt jelenti, hogy senki sem kötelezhető arra, hogy önmagát terhelő vallomást tegyen vagy önmaga ellen bizonyítékot szolgáltasson.[70]

A megoldást azokban az esetekben, amikor a hatóság hozzáfér a privát kulcshoz, az jelentené, ha rendelkezne egy hatósági címmel, amelyre át kellene utalni a lefoglalás foganatosítása során a *kriptovalutákat. Szathmáry* ezt „kikényszerített

[65] Department of Justice, U.S. Attorney's Office, Southern District of New York, 2017. 09. 29. https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins; illetve a CNN híre, 2018. 05. 28., https://www.ccn.com/london-police-seize-500000-in-bitcoin-from-cybercrime-wave-hacker/ (2019. 01. 21.).

[66] A Koreatimes híre, 2018. 05. 30. http://www.koreatimes.co.kr/www/biz/2018/05/488_249868.html (2019. 01. 21.)

[67] Be. 308. § (3).

[68] Czine Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): *Büntetőeljárás jog I–II. – új Be. – Kommentár a gyakorlat számára.* HVG-ORAC, Budapest, 2018, HVG-ORAC Jogkódex; valamint Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi Szemle,* 2018/2, 126.

[69] A kriptovaluták lefoglalásának részleteire lásd Halász Viktor: A Bitcoin működése és lefoglalása a büntetőeljárásban. *Belügyi Szemle,* 2017/7–8, 128–146.

[70] Be. 7. § (3).

tranzakciónak" nevezi.[71] Ezáltal tud teljes mértékben megvalósulni a vagyoni érték feletti rendelkezési lehetőség akadályozása.[72] Erre utal a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló 11/2003. (V. 8.) IM-BN-PM együttes rendelet 67. § (5) bekezdése, amely szerint *„az elkobzás vagy vagyonelkobzás alá eső fizetésre használt elektronikus adat lefoglalását a Be. 315. § (2) bekezdésében meghatározott művelet elvégzésével, a fizetésre használt elektronikus adat áthelyezésével vagy az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával kell végrehajtani, ha a) az adat vagyonelkobzás alá esik, és a zár alá vétel feltételei nem állnak fenn, vagy az nem lenne végrehajtható, illetve b) az adat elkobzás alá esik, és az elektronikus adat ideiglenes hozzáférhetetlenné tételének vagy az elektronikus adat ideiglenes eltávolításának a feltételei nem állnak fenn".* A Be. 315. § (2) bekezdésében meghatározott művelet elvégzése végrehajtható olyan művelettel is, amely alapján a fizetésre használt elektronikus adat értéke a bűnjelkezelő e célból rendszeresített számláján kerül jóváírásra. A fizetésre használt elektronikus adat vagyonelkobzás érdekében történő lefoglalását követően haladéktalanul fel kell hívni az érintettet, hogy a bűnjel előzetes értékesítése vagy megváltása kérdésében nyilatkozzon. Amennyiben az érintett kéri a fizetésre használt elektronikus adat értékesítését, ez csak abban az esetben mellőzhető, ha arra a bizonyítás érdekében is szükség van. Ha a fizetésre használt elektronikus adat lefoglalását a 67. § (5) bekezdésében meghatározott módon hajtják végre, és annak a bírósági bűnjelkezelő rendelkezésére bocsátása szükséges, azt az ügyészség vagy a nyomozó hatóság a bírósági bűnjelkezelő e célból rendszeresített számláján történő jóváírással teljesíti.

A hatósági felügyelet alatt álló *kriptovaluták* biztosítása is fontos, különösen a hatósági visszaélések elkerülése érdekében. Például a nyomozók a *Silk Road ügy* során lefoglalt *bitcoin*-egységeket lopták el a hatósági pénztárcából.[73] Éppen ezért a hatósági tárcának a legalkalmasabb az ún. *multisig* vagy *multisignature* tárca típus, amely csak akkor engedélyezi a *kriptovaluták* küldését, ha az előre megadott kulcsok közül a meghatározott számú privát kulccsal igazolást kap. Ezt a rendszert bármilyen kombinációban ki lehet alakítani a felek megegyezése szerint.[74]

3. Összefoglalás

Összességében elmondható, hogy a *kriptovalutákkal* való visszaélések tekintetében általában nem is a bűncselekmény helyes minősítése okozhat problémát a gyakorlatban, hanem az, hogy az elkövetés tárgyát hogyan sorolhatjuk be jogi szempontból.

[71] Szathmáry (2015): i. m., 646.

[72] Szathmáry (2015): i. m., 646.

[73] A Reuters híre, 2017. 11. 08. https://www.reuters.com/article/us-usa-cyber-silkroad/ex-agent-in-silk-road-probe-gets-more-prison-time-for-bitcoin-theft-idUSKBN1D804H (2019. 01. 12.).

[74] Furneaux, Nick: *Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence*. Wiley, 2018, 71. (https://doi.org/10.1002/9781119549314).

Előrelépés, hogy az ötödik pénzmosás elleni irányelv meghatározta a virtuális fizetőeszközök fogalmát. Továbbá az Unióban felismerték, hogy a *kriptovaluták* használata és a különböző átváltó, valamint pénztárca-szolgáltatók szolgáltatásainak igénybevétele pénzmosási és terrorizmus-finanszírozási kockázatot hordoz magában. Ezért az irányelv hatályát már e szolgáltatókra is kiterjesztették, és nekik is meg kell felelniük a szigorúbb pénzmosás elleni, avagy „ismerd meg az ügyfeledet" szabályoknak. Ezen kívül a 2019-es irányelv, felismerve a virtuális fizetőeszközök használatában rejlő veszélyeket – különös tekintettel a számítógépes csalásra –, rögzíti, hogy az immateriális készpénz-helyettesítő fizetési eszközök körében büntetőjogi védelmet kell biztosítani a digitális pénztárcáknak is, amelyekkel az egyes pénzbeli értékkel rendelkező *kriptovaluták* utalhatók.

A hazai szabályozás vizsgálata alapján megállapítható, hogy különösen a pénzmosás tényállása világít rá arra, hogy e deliktum elkövetési tárgyát, a bűncselekményből származó „dolog" fogalmát értelmező rendelkezés keretében ki kellene terjeszteni a *kriptovalutákra* is. Továbbá a jognak nemcsak a *kriptovalutát,* hanem a kapcsolódó egyes tevékenységi köröket is szabályoznia kell, mint például az átváltó-, befektetési és pénztárca-szolgáltatókét a pénzügyi vagy kiegészítő pénzügyi szolgáltatások keretében, amelyhez a háttérjogszabály módosítása szükséges. Ez azonban – hasonlóan a *kriptovaluták* jogi besorolásához – elsődlegesen nem a büntetőjog feladata.

Abstract

The legal status of cryptocurrencies is a gray area in most legal systems. Although criminals increasingly abuse cryptocurrencies to fund criminal activities. The study analyses solely the criminal use of cryptocurrencies. For example money launderers have evolved to use cryptocurrencies in their operations, therefore legislative changes at EU level, or the uniform application of existing anti-money laundering regulations have been required. In a trend mirroring attacks on banks and their customers, cryptocurrency users and exchangers have become victims of cybercrimes themselves. Conventional crimes may be committed via cryptocurrencies such as fraud and extortion. Darknet criminal markets use cryptocurrencies as payment instruments since they offer better anonimity and some of them greater privacy. They are less traceable and their decentralised system challenges the law enforcement.